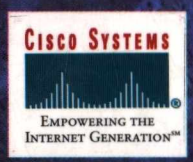
Cisco Systems:
Світовий лідер мережевих вирішень Internet

Є. Буров

Комп'ютерні мережі



Євген Буров

Комп'ютерні мережі

За редакцією проф. В.Пасічника

Львів – 1999

ББК 32.97
УДК 681.324

Б 916 **Буров Є.**
Комп'ютерні мережі. Львів: БаК, 1999. - 468 с., іл.
ISBN 966-7065-19-7

У цьому фундаментальному виданні висвітлено практично всі сучасні мережеві інформаційні технології. Розглянуто апаратні та логічні принципи побудови мереж, функції протоколів, сучасні комерційні технології локальних та глобальних мереж, питання керування та адміністрування мережами, об'єднання мереж, віддаленого доступу, архітектур розподілених обчислень. Значну увагу приділено побудові коректних мережевих вирішень, наведено типові вирішення. Порівняно мережеві функції головних мережевих операційних систем.

Це унікальне за інформаційною насиченістю видання можуть використовувати як студенти, так і спеціалісти в галузі інформаційних технологій.

Науковий редактор
канд.техн.наук О.Коссак

Редактор
М.Мартиняк

ISBN 966-7065-19-7

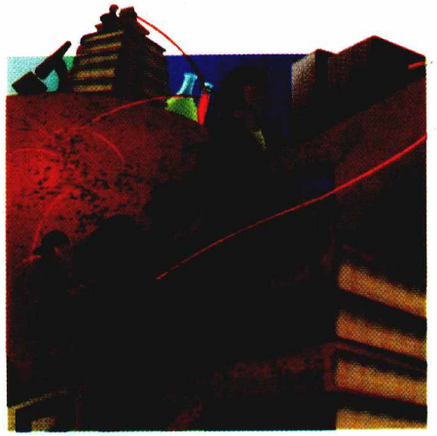
Компанію заснувала наприкінці 1984 року мала група вчених-комп'ютерників Стенфордського університету, які шукали простішого способу об'єднання різних типів комп'ютерних систем. Cisco System випустили свою першу продукцію в 1986 році. Відтоді Cisco стала транснаціональною корпорацією, понад 16000 службовців якої працюють у 200 офісах 55 країн.

Електронною поштою пересилають удесятеро більше листів, ніж звичайною

Понад 200 років тому промислова революція глибоко вплинула на світову економіку. Сьогоднішня Internet-революція матиме всесвітній вплив значно більших розмірів і змінить долю компаній, країн і людей. Internet змінює спосіб праці, життя, розваг і навчання, надає можливості, які ми тільки починаємо усвідомлювати. Ці зміни утворюють нову Internet-економіку, де технологія єднає кожного з усім, де домінують відкриті комунікації, відкриті стандарти і відкриті ринки.

Щосекунди до Internet'у долучається семеро нових користувачів

Internet фундаментально змінив спосіб спілкування. Люди всього світу, використовуючи Internet, навчаються, купують подарунки, листуються зі своїми родичами і друзями, планують відпочинок і навіть купують собі автомобілі. Internet втілює Internet-економіку, яка охоплює будь-яку групу людей, компаній чи країн. Internet досяг більшого і значно швидше, ніж будь-яка попередня технологія зв'язку. Наприклад, для радіо потрібно було 35 років, щоб охопити 50 млн. слухачів, телебаченню - 13 років. Internet досяг цього за 4 роки. Сьогодні діловий, урядовий та освітній сектори використовують Internet, змінюючи стиль своєї



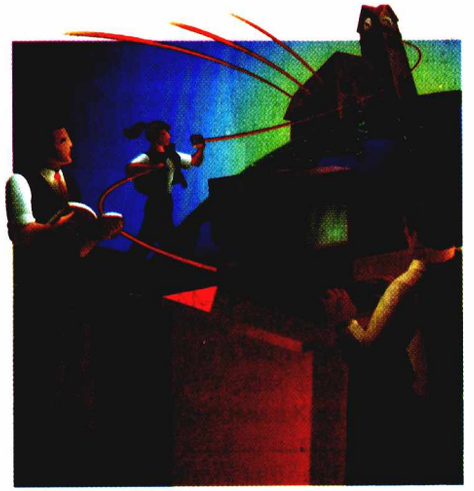
роботи шляхом збільшення інвестувань у мережеві технології. Наприклад, багато підприємців у сфері роздрібної торгівлі трансформувалися і використовують Internet для організації торгівлі й обслуговування клієнтів через мережі. Впровадження цифрових інформаційних технологій збільшує сфери впливу і доходи компаній, що застосовують Internet. Оскільки накладні витрати мінімальні, то вироби і послуги стають відповідно значно дешевшими. Крім того, уряди використовують Internet для спілкування зі своїми громадянами та удосконалення управління. Навчальні заклади приєднуються до Internet: стає можливим як дистанційне навчання студентів, так і доступ до інформаційних ресурсів учням будь-якого віку. Компанії і країни, які успішно застосовують Internet-економіку, легко і безперервно реагують на ринкові зміни і вимоги клієнтів. Споживачі, постачальники, службовці і ділові партнери можуть разом співпрацювати, що дає змогу підвищити продуктивність, швидко адаптуватися до змін і приймати ефективні рішення. Мережа є головним двигуном нового світу Internet.

Якогось дня Internet цілковито витіснить міжміські телефонні розмови

Виникнення мереж та Internet змінюють спосіб праці, життя, розваг і навчання, і Cisco Systems робить ці зміни можливими.

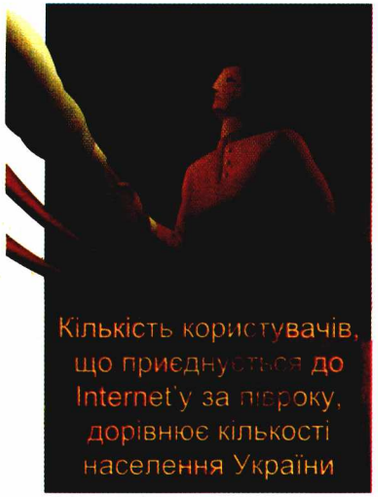
Кожного дня Cisco та її клієнти підтверджують, що мережеві технології можуть фундаментально і вигідно змінити спосіб і діловий стиль роботи компаній.

У багатьох випадках сама Cisco є найліпшим прикладом компанії, яка використовує Internet-технологію, щоб мати стійку перевагу над конкурентами. Сьогодні клієнти, службовці, акціонери, ділові партнери і постачальники застосовують наш визнаний Web-сайт, щоб одержати інформацію, звертатися за підтримкою,

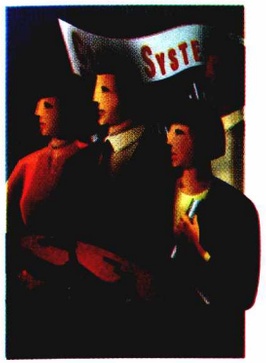


укладати угоди, розміщати замовлення. Тепер Cisco має один з найбільших у світі сайтів електронної торгівлі. Минулого року понад 64% послуг Cisco і приблизно 73% замовлень її клієнтів були проведені через Web. Використовуючи мережеві застосування, Internet і свою власну мережу, Cisco економить щорічно понад 320 млн. доларів накладних видатків, одночасно поліпшуючи взаємини з клієнтами та партнерами, і досягає переваги над конкурентами в таких сферах, як обслуговування клієнтів, замовлення виробів і швидкість постачання.

Cisco продає свою продукцію в 90 країнах світу через власну мережу збуту, системних інтеграторів, дистрибюторів і партнерів.



Партнери Cisco Systems в Україні



Атлас
вул. Грушевського, 30/1
Київ 252021
тел.: (044) 253 21 73
факс: (044) 253 34 36

INT
вул. Січневого повстання, 13
Київ 252010
тел.: (044) 290 74 31
факс: (044) 290 89 34

Soft-tronic
вул. Лескова, 9
Київ 252011
тел.: (044) 294 88 21
факс: (044) 294 89 31

S&T
вул. Попудренка, 50
Київ 253094
тел.: (044) 513 60 20
факс: (044) 559 50 33

Представництво Cisco Systems в Україні

вул. Шовковична, 42-44, Київ 252004; тел.: (044) 490 12 06: факс: (044) 490 12 00

http://www.cisco.com

Cisco Systems
Empowering the Internet Generation℠

Райхле і Де-Массарі Україна

R&M

бул. Лихачова, 1/27
Київ 252133
Тел./факс:(044) 295 69 69
E-mail: rdm@rdmua.com.ua
Internet: http://www.rdm.ch

вул. Сонячна, 5
Одеса 270009
Тел.: (0482) 60 45 51
(0482) 60 45 52
Факс: (0482) 21 99 88
E-mail: rdmua@farlep.net

ФІРМА РАЙХЛЕ І ДЕ-МАССАРІ (R&M) ТА СПЕКТР ЇЇ ОБЛАДНАННЯ

Портрет фірми

Фірма REICHLE&DE-MASSARI AG (Швейцарія, Ветцікон, далі **R&M**) заснована тридцять п'ять років тому. Сьогодні це одна з провідних фірм-виробників у галузі інформаційної техніки і техніки зв'язку.

Фірма **R&M** має десять дочірніх підприємств, виробляє і збуває продукцію на національному та міжнародних ринках у понад 100 країнах світу. **R&M** відома як підприємство з дуже високим технічним і технологічним рівнем, що підтверджено міжнародним сертифікатом якості ISO 9001. Чимало технологій запатентовані і не мають аналогів у світі.

На світовому ринку фірма **R&M** спеціалізується з виробництва техніки зв'язку, передавання даних і випускає повну гаму виробів для введення, сполучення, комутації, передавання і розподілу інформації по мідних і оптичних кабелях, виконує програмне забезпечення розробок, технічне обслуговування і менеджмент. Серед офіційних бізнес-партнерів фірми такі відомі виробники телекомунікаційного обладнання, як IBM, SIEMENS, Lusent Technologies, KAPSCH, NEC та ін.

Тепер фірма розгортає роботу на ринках Східної Європи, де відбувається масова реконструкція телекомунікаційних мереж. Саме тут передові технології фірми дали змогу потіснити конкурентів і мати успіх на ринках Польщі, Угорщини, Словаччини, Чехії, Росії та інших країн.

Початком роботи на українському ринку стало отримання фірмою **R&M** сертифікатів Міністерства зв'язку України на весь спектр продукції (Сертифікати № 241, 242, 243, 244, 245, 246 від 14 грудня 1995 року). У квітні 1997 року в Україні зареєстроване дочірнє підприємство – фірма Райхле і Де-Массарі Україна з офісами в Києві та Одесі.

Оптимальні вирішення для Ваших кабельних мереж

Це дало змогу фірмі розгорнути активнішу діяльність на українському телекомунікаційному ринку стосовно не лише організації мережі збуту продукції, а й виробництва різних компонент.

Спектр виробів фірми R&M

Для вирішення проблем, пов'язаних з побудовою сучасної, гнучкої і надійної розподільної системи з високою якістю з'єднань, **R&M** пропонує широкий спектр обладнання.

З метою розумного вкладення коштів та їх максимальної віддачі фірма розробила дві технології в галузі кросового і розподільного обладнання для мідних кабелів. Дешевші і простіші технології *VS-Стандарт/VS-Компакт* рекомендовано застосовувати у системах невеликої ємності, коли обслуговування і роботу з кросовим господарством ведуть нерегулярно (ПСК, УПАТС тощо). Дорожчу й унікальну технологію *VS-Модуляр* ліпше використовувати на великих станційних кросах і розподільних шафах, з якими працюють щоденно, а обслуговування потребує максимальної гнучкості і зручності. Саме ця технологія завдяки модульній конструкції плінта дає змогу замінювати старе обладнання на нове без розірвання зв'язку. Будь-яку із зазначених технологій можна легко адаптувати до вже наявних у мережі металевих конструкцій старих кросів, що полегшує перехід і знижує витрати у разі переходу від старих технологій до нових. У рамках застосування зазначених технологій **R&M** пропонує такий спектр обладнання:

– кросове обладнання в настінному, настінно-підлоговому, вертикальному, вертикально-горизонтальному виконанні з фальшпідлогою або без неї;

– чотири типи модулів для монтажу на кросі: з'єднувальний, роз'єднувальний постійно замкнутий, роз'єднувальний постійно розімкнутий і заземлювальний;

– розподільні шафи і кінцеві бокси для тривалого використання зовні приміщень у будь-якій кліматичній зоні;

– розподільні бокси і короби для використання всередині приміщень з гнучким розміщенням.

У галузі розподільного обладнання для волоконно-оптичних кабелів **R&M** пропонує:

– кінцеві і проміжні бокси, що підтримують усі наявні типи з'єднань для одно- та багатомодового волокна;

– оптичні муфти (прохідні і тупикові) будь-яких розмірів і ємності;

– оптичні кроси 19" стандарту з компактними і багатофункціональними модулями;

– супутнє периферійне і допоміжне обладнання для монтажу і подальшого обслуговування.

Структуровані кабельні системи R&M freenet

Структуровані кабельні мережі стають щораз актуальнішими. Без них не можна побудувати надійні, гнучкі й високошвидкісні мережі передавання мовлення, даних і відео для сучасного підприємства будь-якого рангу – офісу, банку чи виробничого підприємства.

Сучасні технології, що розвиваються (*FDDI, ATM, Fast Ethernet, 1000BASE-T* та ін.), ставлять щораз жорсткіші вимоги до первинних мереж, у яких використовують мідні й оптичні кабелі. Це зумовило розвиток відповідних технологій, стандартів і норм для кабельних мереж, і, отже, всіх пасивних компонентів, на яких такі мережі будують.

Структурована кабельна система – це технологія, яка дає змогу оптимально і швидко побудувати кабельну мережу підприємства з можливістю нарощувати її в майбутньому без глобальних змін у наявній інфраструктурі та з мінімальними витратами.

Однією з перших фірм, що пропонують свою структуровану кабельну систему і випускають увесь спектр потрібного обладнання для її побудови, є фірма **REICHLE+DE-MASSARI** (Швейцарія, Ветзікон), удостоєна міжнародного сертифіката якості **ISO 9001**.

Сьогодні фірма пропонує вирішення в рамках нової системи **1998** року **R&M FreeNet,** які дають змогу будувати кабельні мережі з перепускною здатністю до **750 МГц**, інтеграцією технологій передавання мовлення та даних і відповідають усім чинним американським, європейським і світовим стандартам.

Нова Структурована кабельна система **R&M freenet** забезпечує комплексне вирішення для побудови найсучаснішої кабельної інфраструктури.

Система складається з компонент Категорій 5e, 6, 7 і волоконно-оптичних (Клас D, E і F); підтримує оптичні і мідні середовища.

Модульний дизайн системи дає змогу легко нарощувати її можливості.

Кольорове маркування призначене для легкої ідентифікації різних сервісів.

Система забезпечує великий резерв щодо продуктивності (ACR), що гарантує роботу майбутніх застосувань.

Спеціальні способи механічного захисту створюють необхідний захист обладнання від несанкціонованого доступу або неправильного увімкнення

Нові з'єднувачі SC-RJ, MT-RJ, LSH(E200) для волоконно-оптичних кабелів стрічкового типу забезпечують високий ступінь інтеграції оптичних портів у СКС і повну взаємозамінність зі стандартним RJ45.

Для прокладання волоконно-оптичних кабелів усередині будинків і безпосередньо до робочого місця фірма розробила унікальні технології **Fiberdesc** і **Fibereasy**, які випереджають розробки найближчих конкурентів мінімум на один рік, а технологія моментального викінчення волокон стандартними ST, SC, SC-RJ і MT-RJ з'єднувачами без застосування клею, яка не потребує полірування, не має аналогів у світі.

Шановний читачу!

Ви розгорнули книгу, яку ще до її виходу в світ фахівці назвали першим україномовним енциклопедичним виданням про комп'ютерні мережі.

Бурхливий потік публікацій з сучасних інформаційних технологій, його насиченість та розмаїття в багатьох виданнях може дезорієнтувати не тільки початківця, а й досвідченого інформатика. Зокрема це стосується сектора мережевих інформаційних технологій.

У пропонованій монографії увагу зосереджено на двох рівнях подання мережних технологій, а саме: телекомунікаційному та комп'ютерному. Книга складається з трьох частин. У першій висвітлено головні принципи організації мереж, середовища передавання, апаратні вирішення, протоколи. Детально схарактеризовано протокольний стек TCP/IP. Другу частину присвячено мережевим технологіям. Розглянуто технології локальних та глобальних комп'ютерних мереж. У третій частині описано головні принципи організації операційних систем комп'ютерних мереж. Розглянуто Windows 95x, Windows NT, Novell Netware, Unix. Кожен з розділів складається з головної частини та додатків. Структурно головна частина розділу призначена для ознайомлення з проблематикою та формування у читача цілісної картини, детальніша ж інформація наведена у додатках. Автор у багатьох випадках подає результати своїх наукових пошукувань, що робить методично коректно. Це дає змогу чіткіше пов'язати розділи і параграфи книги. Хочу звернути увагу читачів книги на глибоке відпрацювання автором понятійно-термінологічного аспекту, який для новітніх галузей науки та технологій є чи не найвразливішим.

Весь матеріал пропонованого видання неодноразово опрацьований під час викладання курсів «Комп'ютерні мережі», «Локальні комп'ютерні мережі» та «Операційні системи комп'ютерних мереж», які читає автор для студентів факу «Інтелектуальні системи прийняття рішень» та інших споріднених базових напрямів та спеціальностей.

Фундаментально-прикладний характер книги дає змогу пророкувати їй ринковий успіх.

Бажаю шановному читачу відшукати в книзі щонайвичерпніші відповіді на всі питання, що його цікавлять, а її автору нових творчих здобутків.

Володимир Пасічник
д-р техн. наук, професор

Від автора

В основі книги є курс лекцій прочитаний у Державному університеті «Львівська політехніка». Ідея її написання виникла як відповідь на розрізненість, несистематизованість інформації з сучасних мережевих технологій, відсутність цілісного викладення базових принципів. Працюючи над курсом лекцій, ми розпочали створювати структуровану інформаційну базу даних з мережевих технологій шляхом узагальнення великої кількості джерел, зіставлення та порівняння технологій. Базу даних постійно поповнюють та актуалізують, а книга є її часовим зрізом.

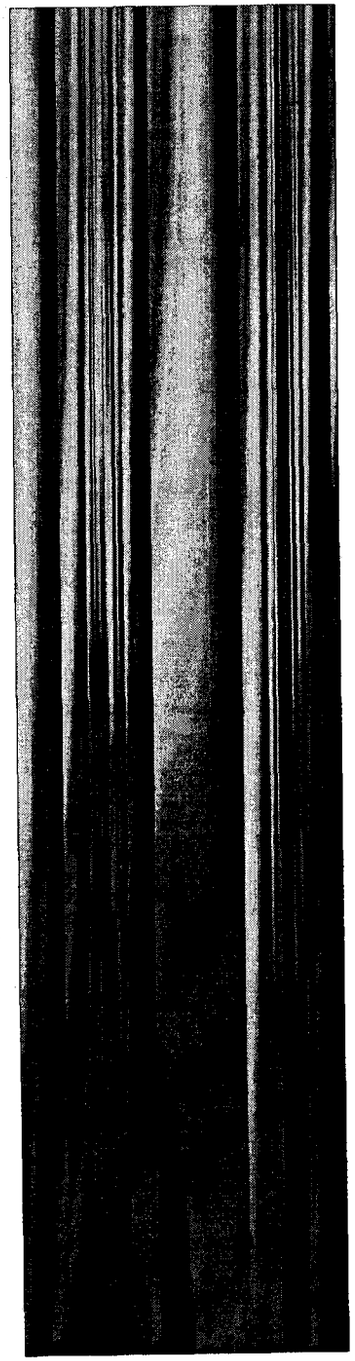
Мета книги – створити в читача цілісну систематизовану картину різних галузей мережевих технологій у їхніх взаємозв'язках та взаємозалежностях.

Головна аудиторія книги – студенти комп'ютерних спеціальностей, тобто люди з певними знаннями про комп'ютери, електроніку, операційні системи, а також спеціалісти та бажаючі. Водночас вона не призначена для 'чайників', не є популярним виданням. Ми ставили за мету висвітити достатньо складні питання, орієнтовані на фахівців, або людей, які бажають стати фахівцями.

Користуючись нагодою, хочу висловити подяку всім, хто сприяв виходу книги в світ: літературному редактору п. М.Мартиняк, видавцю п. О.Коссаку, які витратили багато зусиль та часу на шліфування мовних та термінологічних аспектів, створенню покажчика та переліку вживаних скорочень, професору В.Пасічнику за цінні поради та допомогу у вирішенні організаційних питань, моїй дружині Оксані за розуміння та підтримку.

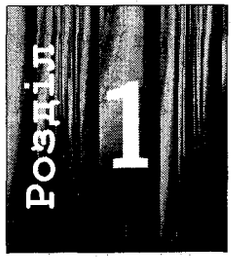
Особлива подяка всім рекламодавцям, а особливо фірмам Cisco Systems та Reichle & De Massari, які надали свої технічні матеріали та забезпечили фінансову підтримку проекту.

У книзі, напевно, є неточності та й матеріал може дещо застаріти в зв'язку з швидкими змінами у мережевих технологіях. Ми будемо вдячні, якщо читач з розумінням поставиться до цього і з радістю приймемо всі зауваження та побажання.



Частина 1

ПРОТОКОЛИ КОМП'ЮТЕРНИХ МЕРЕЖ



ІСТОРІЯ РОЗВИТКУ ТА КЛАСИФІКАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Історія виникнення та техніко-економічні передумови появи комп'ютерних мереж. Різновиди комп'ютерних мереж. Діаграма швидкість–відстань передавання. Локальні та глобальні мережі. Їхні відмінності. Розподілені інформаційні системи. Регіональні та корпоративні мережі. Класифікація комп'ютерних мереж. Стандартизація в комп'ютерних мережах.

1.1. Історія виникнення та техніко-економічні передумови появи комп'ютерних мереж

З глибокої давнини людство намагалося винайти засоби організації зв'язку на далеку відстань. До таких засобів можна віднести димовий телеграф, там-тами, сигнальні вогні та ін. Безпосереднім провісником сучасних комп'ютерних мереж (КМ) були телеграфна та телефонна мережі XIX ст. Створення мереж передавання даних та розподіленого їх опрацювання було результатом науково-технічної революції та розвитку мікроелектроніки. Ще в 50-х роках XX ст., коли з'явилися досить потужні ЕОМ, виникла потреба сполучати їх з одним або багатьма терміналами для ефективнішого використання їхніх ресурсів. Було створено системи з розподілом часу роботи центрального процесора, де кожному терміналу по черзі виділявся квант часу. Така структура системи телеопрацювання даних показана на рис. 1.1.

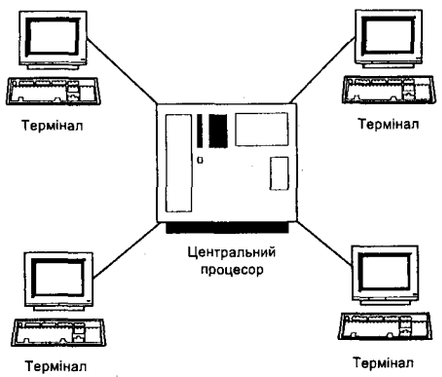


Рис. 1.1. Початкова структура системи телеопрацювання даних.

Канали зв'язку в такій системі були досить дорогими і використовувалися терміналами неефективно. Тому згодом учені розробили спеціальні пристрої (мультиплексери та концентратори), які збирали трафік (інформаційні потоки) з розташованих поблизу терміналів для спрямування його до центрального процесора (ЦП). Елементом такої системи також був фронтальний процесор, який виконував функції організації зв'язку (рис. 1.2).

Унаслідок еволюції мережа поступово набула свого сучасного вигляду (рис. 1.3). Тепер вона має не один, а багато центральних процесорів, терміналів та мережу зв'язку, яка складається з вузлів. Кожен вузол мережі – це спеціалізована на виконанні комунікаційних функцій ЕОМ (маршрутизатор). Для передавання даних між вузлами використовують призначені канали наявної телефонної мережі. Замість терміналів щораз частіше використовують персональні комп'ютери.

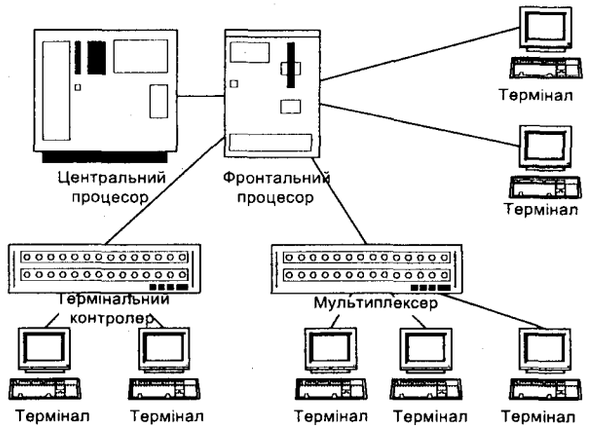


Рис. 1.2. Структура системи телеопрацювання з фронтальним процесором.

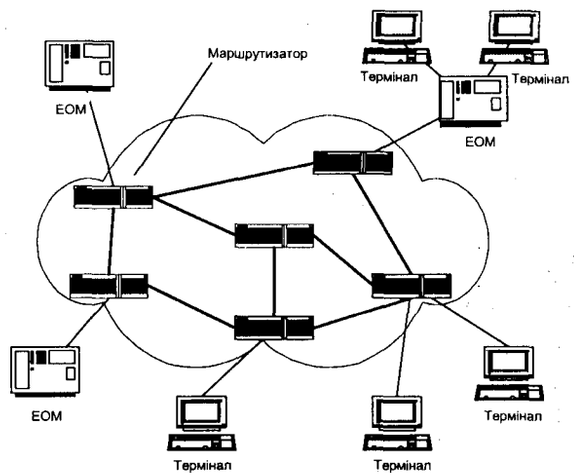


Рис. 1.3. Структура сучасних глобальних мереж.

Поряд зі створенням глобальних мереж науковці намагалися організувати передавання даних у локальній зоні. Це зрозуміло, адже, за результатами аналізу, понад 80% інформаційних потоків концентрується в локальній зоні – у межах відділу, організації, підприємства (правило 80–20). У 80-х роках були спроби організувати зв'язок між машинами на рівні одного підприємства з використанням місцевої АТС. Однак справжній розвиток локальних мереж розпочався завдяки появі дешевих мікропроцесорів та персональних ЕОМ. Масове використання мікропроцесорів у вузлах та пристроях (так званого розподіленого інтелекту), а також персональних ЕОМ спонукало організувати надійний зв'язок між ними для сумісного розв'язування задач та використання ресурсів. З появою персонального комп'ютера стало можливим наблизити місце опрацювання інформації до місця її виникнення і таким чином збільшити ефективність роботи інформаційної системи.

1.2. Різновиди комп'ютерних мереж

Найліпше проілюструвати місце та співвідношення різних видів КМ серед систем телеопрацювання даних можна за допомогою діаграми "швидкість – відстань передавання" (рис.1.4). По осі ординат цієї діаграми відкладено швидкості передавання, а по осі абсцис – відстань, на яку воно виконується.

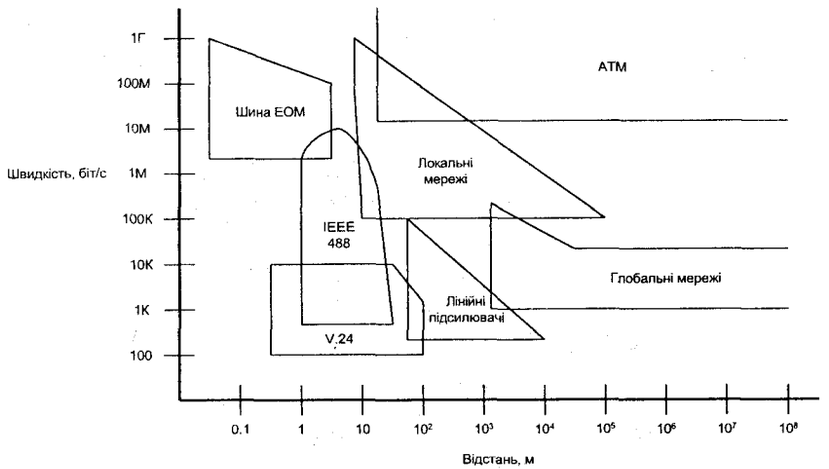


Рис. 1.4. Діаграма "швидкість – відстань передавання".

На діаграмі показано такі системи телеопрацювання даних: шина ЕОМ (забезпечує дуже високі швидкості передавання даних (> 100 Мбіт/с) на короткі відстані (1–10 м)), система передавання даних стандарту IEEE-488 (гарантує швидкісне передавання даних для лабораторної апаратури (швидкість передавання до 10 Мбайт/с, дальність – від 1 до 10 м)), рекомендації

V.24 (визначають швидкісні характеристики інтерфейсу термінала з модемом), лінійні підсилювачі (дають змогу терміналам приєднатися до ЕОМ через скручену пару на відстані до декількох кілометрів, але з обмеженою швидкістю). Глобальні мережі загального користування охоплюють усю земну кулю, але мають малу швидкість передавання даних. Наприклад, тривалість передавання одного інформаційного пакета в глобальній мережі становить кілька секунд, а в локальній – кілька мілісекунд.

Отже, з усіх засобів телеопрацювання сьогодні можна виділити два типи мереж, що суттєво відрізняються за технологічними вирішеннями: **локальні інформаційні мережі (ЛМ)** та **глобальні інформаційні мережі (ГМ)**. В англомовній літературі для них використовують відповідно терміни **Local Area Network (LAN)** та **Wide Area Network (WAN)**.

• ***Локальні інформаційні мережі.*** За допомогою ЛМ інформацію передають на невелику відстань. Однією з визначальних ознак ЛМ є наявність високошвидкісного каналу передавання даних, швидкість у ньому на порядок вища, ніж швидкість периферійних пристроїв комп'ютерів, та наближається до швидкості внутрішньої шини комп'ютера. Тому в деяких популярних виданнях ЛМ трактують як комп'ютер з комп'ютерів. Наявність швидкісного каналу дала змогу створити на базі ЛМ єдину цілісну інформаційну систему, в якій витрати часу на зв'язок суттєво не впливають на час виконання функцій. Таку систему телеопрацювання даних називають *розподіленою*. Оскільки головним завданням такої системи є опрацювання інформації, її ще називають **розподіленою інформаційною системою (РІС)**. У РІС реалізовано новий (не фон-Нейманівський), паралельний порядок опрацювання інформації, що створює нові можливості для підвищення потужності та ефективності інформаційних систем. А це ставить перед ученими та інженерами нові теоретичні та практичні проблеми. Науковці виділяють три ступені використання РІС.

1. *Розподіл ресурсів.* Задачі сумісно використовують ресурси системи (пам'ять, дискові накопичувачі, принтери). Таке використання РІС сьогодні найпоширеніше.
2. *Розподіл навантаження.* Задачі, які надходять у систему, передаються на вільні ЕОМ.
3. *Розподілене опрацювання даних.* Сукупність елементів опрацювання, пов'язаних логічно та фізично децентралізованим керуванням ресурсами з метою сумісного виконання прикладних програм. Елементи розподілу навантаження та розподіленого опрацювання даних реалізовані в нових версіях операційних систем Netware, Unix, Windows NT.

У локальних мережах найдорожчими є пристрої опрацювання інформації, а не комунікації. Ефективність системи ЛМ можна підвищити, якщо головну увагу приділити ефективному використанню прикладної частини (апаратура+програми+персонал).

• **Глобальні інформаційні мережі.** ГМ територіально не обмежені. Для передавання даних у ГМ найчастіше використовують наявні телефонні канали з малою швидкістю передавання (≈1–3 Кбіт/с) та великим впливом завад. Тому вислідна швидкість передавання в ГМ, як уже зазначалося, невелика. Це унеможливлює використання ГМ у реальному масштабі часу. Тому й не дивно, що найчастіше ГМ сьогодні застосовують для вирішення завдань, які не потребують оперативності (електронна пошта, електронні довідники тощо).

З економічного погляду найдорожчий компонент ГМ – обладнання зв'язку. Для ефективнішого використання системи зв'язку в ГМ застосовують спеціальні процесори зв'язку. Розбіжність між локальними та глобальними мережами в майбутньому можна буде ліквідувати за допомогою **АТМ технології передавання даних** (див. розділ 29).

• Крім локальних та глобальних, виділяють **регіональні мережі** (Metropolitain Area Networks (**MAN**)) – мережі масштабу міста, району, області. Залежно від конкретної реалізації ці мережі можуть базуватися на технології локальних (FDDI) або глобальних мереж.

• Останнім часом, у результаті розвитку мережевих технологій та об'єднання окремих локальних мереж великих фірм у єдине ціле, виникло поняття **корпоративних (територіальних) мереж**. Корпоративна мережа – це об'єднання деякої кількості ЛМ за допомогою телефонних, супутникових, Т1 або інших каналів ГМ у єдину мережу фірми.

1.3. Класифікація комп'ютерних мереж

Ознаки, за якими класифікують комп'ютерні мережі, можуть бути такі:

• *географічна площа* – локальні, регіональні, глобальні мережі;

• *сфера застосування* – офісні, промислові, побутові мережі;

• *комплекс архітектурних вирішень*, що виражається у фірмовій назві – Ethernet, Token Ring, Arcnet;

• *топологія* – шинна, кільцева, зіркоподібна, деревоподібна, повнозв'язна мережі;

• *фізичне середовище передавання* – мережа з симетричним, коаксіальним, волоконно-оптичним кабелем, інфрачервоним, мікрохвильовим каналом, скрученою парою;

• *метод доступу до фізичного середовища* – мережі з опитуванням, маркерним доступом, суперництвом, уставлянням регістра;

• *набір протоколів (протокольний стек)* – мережі TCP/IP, SPX/IPX.

1.4. Стандартизація у комп'ютерних мережах

Характерною особливістю науки про розподілені інформаційні системи є тенденція до стандартизації та формалізації матеріалу. До цього спонукає предмет дослідження: для того, щоб розподілені системи могли нормально функціонувати, усі складові частини повинні працювати за однаковими правилами.

Міжнародний консультативний комітет з телеграфії та телефонії (МККТТ) (Consultative Comittee on Telegraphy and Telephony (**CCITT**)) був створений у 1957 р. У 1993 р. його реорганізували в **Міжнародний Телекомунікаційний Союз (МТС)** (International Telecommunication Union (**ITU**)). Стандарти ITU поділяють на серії. Кожна серія присвячена конкретній тематиці і позначена великою латинською літерою. Наприклад, літерою V позначені стандарти передавання даних по телефонних каналах, літерою X – стандарти мереж передавання даних, літера Q означає стандарти телефонної комутації та сигналізації. Стандарти ITU позначають **S.NNN**, де S – літера серії, а NNN – номер стандарту. Приклади позначень стандартів ITU: X.21, V.42, X.400, X.500. Інколи до позначень стандартів додають суфікси **bis**, **terbo**, наприклад V.42bis. Стандарти з такими суфіксами не мають прямого зв'язку зі стандартами 'без суфікса'. Застосування суфіксів у позначеннях зумовлене вузькістю простору імен.

У 1977 р. при **Міжнародній організації зі стандартизації** (International Standard Organisation (**ISO**)) був організований технічний комітет 97, який розробляє стандарти для опрацювання інформації на ЕОМ. Стандарти цієї організації позначені **NNNN ISO**, де NNNN – номер стандарту. Наприклад: 7498 ISO.

Деякі організації розробляють стандарти певного технологічного напряму або мережі. До таких організацій належать **Комісія з питань діяльності Internet** (Internet Activities Board (IAB) – розробляє питання стандартизації діяльності Internet), **Форум АТМ** ((ATM Forum) – розробляє комплекс стандартів з технології АТМ).

Інформація щодо інших організацій, стандарти яких ми розглядатимемо, наведена в табл. 1.1.

Таблиця 1.1. Деякі організації, що розробляють стандарти КМ

Скорочення	Назва повністю		Приклади позначень стандартів
	по-англійськи	по-українськи	
IEEE	Institute of Electronical and Electrotechnical Engineers	Інститут інженерів електроніків та електротехніків	IEEE-802.1
ECMA	European Computers Manufacturers Association	Європейська асоціація виробників комп'ютерів	ECMA-72, ECMA-81
EIA	Electronic Industries Association	Асоціація електронної промисловості	EIA RS-232C
ANSI	American National Standard Institute	Американський національний інститут стандартів	ASCII
IETF	Internet Engineering Task Force	Підрозділ інженерних розробок Internet	RFC-1231

Бібліографія та джерела

1. *Вейцман К.* Распределенные системы мини и микро ЭВМ / Пер. с англ. М.: Финансы и статистика, 1982.
2. *Федоров А.М.* ITU вчера и сегодня // Сети. 1995. № 3.
3. *Флинт Д.* Локальные сети ЭВМ. Архитектура, принципы построения, реализация / Пер. с англ. М.: Финансы и статистика, 1986.
4. *Frish I.T.* Local area networks – problems and solutions // Proceedings IEEE. Integrated large-scale systems symposium. 1982.

АРХІТЕКТУРНІ ПРИНЦИПИ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

Структура відкритої інформаційної мережі. Стандарт 7498 ISO. Принципи організації середовища зв'язку відкритих систем. Головні функції протоколу N-рівня. Призначення протокольних рівнів стандарту 7498 ISO. Дво- та багатопунктове сполучення. Методи комутації, їхня порівняльна характеристика та застосування.

2.1. Головні означення та поняття

Термінологія в науці про комп'ютерні мережі ще не усталена. Окремі терміни означені стандартами ISO, ITU, IEEE. У нових стандартах уводять нові терміни. Зі спеціальних термінологічних словників, що вийшли останнім часом, можна рекомендувати [1, 3, 4]. Наведемо низку означень, які ми використовуватимемо в подальшому.

• **Реальна система** (real system) – *це сукупність однієї або кількох ЕОМ, відповідного програмного забезпечення, периферійного обладнання, терміналів, персоналу, яка є повністю автономною й опрацьовує та передає інформацію.*

Якщо система не приєднана до мережі, то її називають автономною.

Рис. 2.1. Загальна структура відкритої інформаційної системи.

• **Реальна остаточна система** (real end system) – *це реальна система, яка виконує в мережі функції станції даних, тобто є джерелом або споживачем інформації.*

• **Відкрита система** (open system) – *це система, яка побудована та функціонує з дотриманням вимог міжнародних стандартів.*

Для зовнішнього спостерігача, приєднаного через мережу до відкритої системи, не є суттєвими апаратні особливості ЕОМ, операційні системи, організація обчислювального процесу в інших реальних остаточних системах. Детальніше поняття відкритої системи описане у розділі 32. Загальний вигляд відкритої системи показано на рис.2.1, де АС – це абонентська система.

• **Комунікаційна система** (communication system) – *це реальна відкрита система, яка забезпечує обмін даними між абонентськими системами у відкритій інформаційній системі.*

• **Абонентська система** (user system) – *це реальна відкрита система, яка є постачальником або споживачем ресурсів мережі, забезпечує доступ до них користувачів і керує взаємозв'язком відкритих систем.*

Ініціаторами та учасниками обміну інформацією в абонентських системах є прикладні процеси.

• **Прикладний процес** (application process) – *це процес у реальній остаточній системі, який опрацьовує інформацію для визначених потреб.*

Прикладні процеси можуть мати різну природу. Прикладами прикладних процесів можна вважати дії оператора за терміналом, програму доступу до бази даних, програму керування технологічним процесом. Зв'язок між прикладними процесами безпосередньо реалізується за допомогою середовища передавання даних.

• **Середовище передавання даних** (transmission medium) – *це сукупність ліній передавання даних та, можливо, іншого обладнання, яке забезпечує передавання даних між станціями.*

Частина прикладного процесу, яка відповідає за організацію зв'язку, називається прикладним об'єктом (рис 2.2).

Між прикладними об'єктами в мережі є сполучення, що пролягає через середовище зв'язку відкритих систем.

• **Середовище зв'язку відкритих систем** (OSI environment) – *це сукупність функцій, які дають змогу реальним відкритим системам виконувати обмін даними відповідно до міжнародних стандартів.*

Структуру середовища зв'язку відкритих систем визначає стандарт 7498 ISO. Середовище має складний набір функцій. Тому, створюючи його, треба дотримуватися ієрархічного підходу, що полягає в таких принципах.

1. Функція передавання дуже складна, тому доцільно роділити її на рівні.
2. Кожен рівень виконує конкретний скінченний набір завдань.
3. Межі між рівнями проводять так, щоб обмін був мінімальним.
4. Рівні описують так, щоб зміна одного рівня не спричинювала зміни інших.

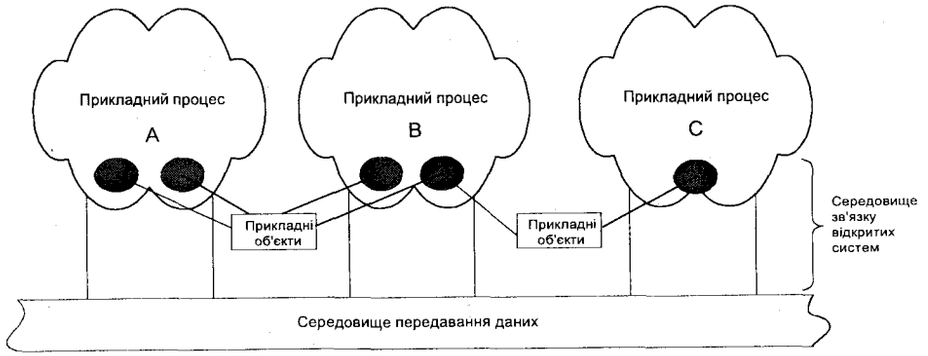


Рис. 2.2. Прикладні об'єкти та середовище зв'язку відкритих систем.

Для локалізації функцій на кожному рівні використовують поняття об'єкта рівня. Підсистема N-рівня може складатися з одного або кількох об'єктів. Між об'єктами одного рівня N у різних реальних системах налагоджується N-сполучення (рис. 2.3). Крім верхнього, кожен N-рівень забезпечує для вищого суміжного з ним N+1-рівня N-послуги. Сукупність послуг N-рівня називається N-сервісом. Якщо якийсь N-об'єкт не в змозі надати послуги, потрібні N+1-об'єктові, він викликає інші N-об'єкти для допомоги, використовуючи сервіс N-1-рівня. Взаємозв'язок між об'єктами одного N-рівня відбувається за допомогою N-протоколів.

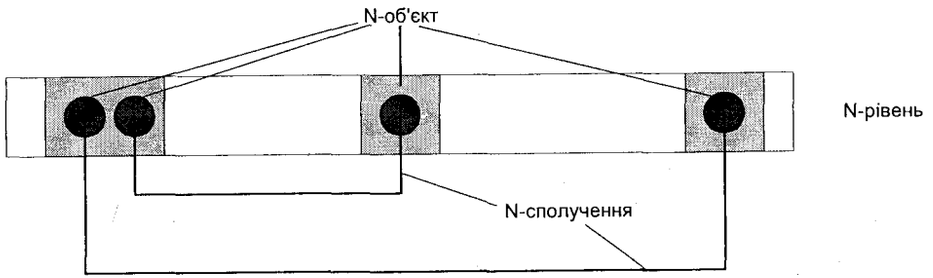


Рис. 2.3. Налагодження N-сполучень.

Протокол – *це набір семантичних та синтаксичних правил, який визначає поведінку об'єктів під час їхньої взаємодії.*

Протоколи намагаються стандартизувати найперше, оскільки об'єкти, пов'язані протоколом, є в різних системах. Об'єкти суміжних рівнів в одній системі взаємодіють один з одним через спільну межу, яку називають інтерфейсом.

Інтерфейс – *це межа між двома рівнями, яка має певні функціональні характеристики.*

Для локалізації тих місць, де надається сервіс, використовують поняття *сервісного пункту доступу* (СПД). У кожний момент часу до N-СПД приєднано тільки один об'єкт N- та N+1-рівня (рис. 2.4). Однак N+1-об'єкт може приєднуватися до різних N-СПД. Кожний N-СПД має свою адресу.

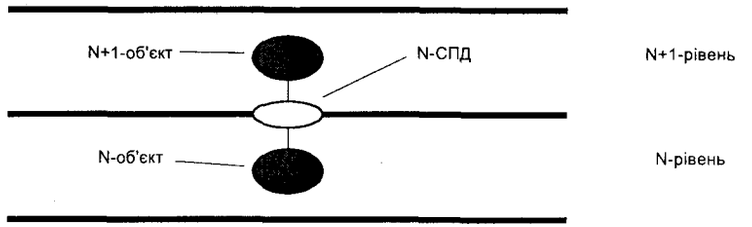


Рис. 2.4. Сервісний пункт доступу.

N+1-об'єкт надає для передавання в N-об'єкт блок даних, який називається *інтерфейсним.* N-об'єкт додає до нього інформацію керування і формує *N-протокольний блок даних.* Інтерфейсний блок даних завжди передається між двома об'єктами двох суміжних рівнів в одній системі, а протокольний блок – між двома об'єктами одного рівня двох різних систем.

2.2. Головні функції протоколу N-рівня

Вибір протоколу. Якщо на N-рівні використовується кілька протоколів, то треба вибрати відповідний.

Налагодження та розривання сполучень. Перед обміном N-об'єкта потрібно сполучитися з відповідним віддаленим N-об'єктом та з'ясувати, чи готовий він до обміну. Сполучення налагоджують за згодою обох об'єктів. Розривати сполучення може N-об'єкт за ініціативою N+1-об'єкта (якщо нормально завершилося передавання) або N-об'єкт за ініціативою N-1-об'єкта (якщо були помилки).

Мультиплексування та розщеплення сполучень. Між N+1- та N-сполученнями може бути кілька співвідношень:

а) одне N-сполучення використовує одне N+1-сполучення;

б) кілька N+1-сполучень використовують одне N-сполучення; у цьому випадку відбувається мультиплексування;

в) одне N+1-сполучення використовує кілька N-сполучень; у цьому випадку відбувається розщеплення.

Передавання даних. Взаємодія реалізується за допомогою N-протокольних блоків даних, які містять N-протокольну інформацію керування та дані користувача, передані N+1-об'єктом. Ці дані передаються прозоро, тобто без зміни їхньої структури та незалежно від неї.

Керування потоком даних. Протокольне керування регулює швидкість обміну між двома об'єктами одного рівня в різних системах, його виконує відповідний протокол. Інтерфейсне керування регулює передавання даних між об'єктами двох суміжних рівнів, його описують локальні домовленості.

Сегментування, блокування, зчеплення даних. Якщо інтерфейсний блок N+1-рівня більший, ніж допустимий розмір протокольного блоку N-рівня, то треба виконати сегментування – розділити блок на частини і розмістити їх у блоках N-рівня. Зчеплення – операція зворотна. Блокування – це функція N-рівня, яка дає змогу об'єднати кілька N+1-блоків в один N-блок (якщо N+1-блоки малі).

Організація послідовності забезпечує на приймальному кінці одержання блоків у такому ж порядку, в якому їх передавали.

Захист від помилок виконують протоколи багатьох рівнів. Він підтверджує правильне передавання, виявляє помилки, повідомляє про них, повертає в початковий стан.

Маршрутизація. Функція маршрутизації на N-рівні забезпечує проходження даних через ланцюжок N-об'єктів. Під час цього процесу за певним алгоритмом будується ланцюжок N-об'єктів, через які послідовно проходить інформація.

Селекція інформації полягає в прослуховуванні каналу і відбиранні з блоків, які проходять через канал, тих, що мають певну адресу.

2.3. Стандарт 7498 ISO

За стандартом 7498 ISO середовище зв'язку відкритих систем поділене на сім рівнів (рис. 2.5).

Рівні 5–7 орієнтовані на обслуговування прикладних процесів, а рівні 1–4 – на надійне передавання даних, тобто на мережу. Функції окремих рівнів показані на рис. 2.6.

Прикладний рівень забезпечує різні форми взаємодії прикладних процесів, розміщених у різних системах. Сьогодні можна виділити такі форми протоколів прикладного рівня:

- керування терміналами;
- керування діалогом;
- керування файлами;
- керування задачами;
- керування системою;
- забезпечення цілісності.

Протокол керування терміналами гарантує приєднання і роботу віддаленого термінала з ЕОМ. Протокол керування файлами реалізує доступ до файлів різних файлових систем. Протокол керування діалогом сполучає процеси та веде діалог між ними. Протокол забезпечення цілісності інформації виявляє помилки, виводить процеси з тупикових ситуацій. Така різноманітність протоколів зумовлена різноманітністю завдань, які вирішують на прикладному рівні. Вибрати потрібний протокол можна динамічно за допомогою спеціального протоколу, який називається *протоколом керування контекстом*.

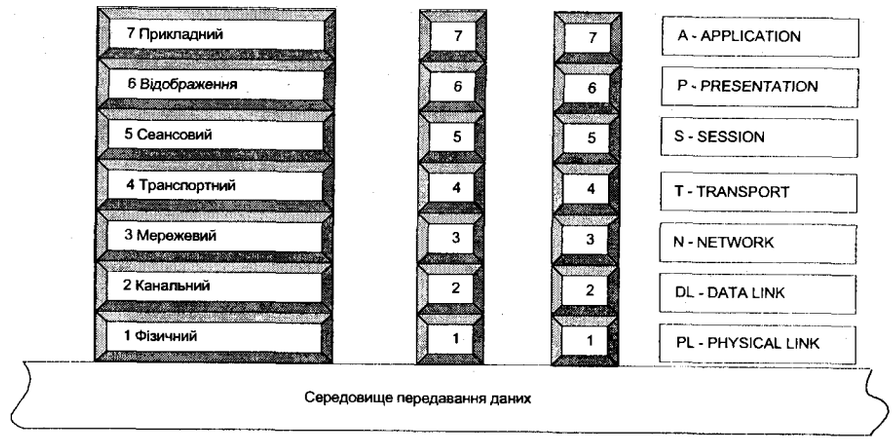


Рис. 2.5. Рівні середовища зв'язку відкритих систем.

Рівень відображення відображає та перетворює дані, якими обмінюються між собою прикладні процеси. Потреба у рівні відображення зумовлена тим, що різні ЕОМ та пристрої, приєднані до мережі, можуть мати різні форми наведення даних: 8, 16, 32, 64-розрядні, різні системи команд та ін. Можна виділити три різні форми відображення даних: ЕОМ – джерела інформації, мережі, ЕОМ – приймача інформації. Рівень відображення призначений для того, щоб спосіб відображення інформації в окремих ЕОМ не впливав на формат інформації в мережі. Кожна інформація, яку формує прикладний рівень для передавання, має два аспекти – семантику і синтаксис. Семантика описує зміст повідомлення і є незмінною. На рівні ж відображення відбувається перетворення синтаксису.

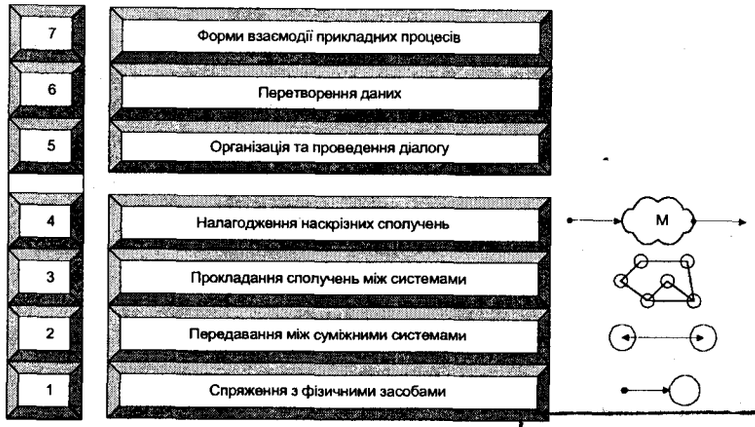


Рис. 2.6. Призначення протоколів усіх рівнів.

Протоколи рівня відображення виконують велику кількість різноманітних функцій, а саме:

- вибір (узгодження між прикладними процесами) потрібної форми відображення даних;
- перетворення даних (кодів, форматів);
- шифрування інформації.

Результат діяльності рівня відображення виявляється під час діалогів (сеансів) об'єктів рівня відображень і узгодження форми подання інформації.

Сеансовий рівень організовує діалогові сеанси між прикладними процесами. Під час роботи сеансового рівня в користувача складається враження, що прикладні процеси розташовані на одному потужному локальному процесорі. Ініціатором сеансу є прикладний об'єкт, який звертається до представницького об'єкта і передає йому адресу партнера. Після цього представницький об'єкт звертається до сеансового й ініціює сеанс зв'язку. Головні функції сеансового рівня такі:

- налагодження сеансового сполучення;
- обмін даними;
- керування взаємодією;
- повідомлення про надзвичайні ситуації;
- відображення сеансового сполучення на транспортне;
- закінчення сеансового сполучення.

Під час *налагодження сеансового сполучення* шляхом діалогу об'єктів вибираються параметри сполучення: швидкість передавання, потреба підтверджень та ін.

Обмін даними – головна функція рівня, яка реалізує передавання інформації між об'єктами сеансового рівня.

Керування взаємодією – це керування черговістю передавання протокольних блоків.

Можлива ситуація, коли через одне транспортне сполучення відбувається передавання інформації з кількох сеансів. Тому кожен сеанс повинен мати ідентифікатор. З іншого боку, інформацію одного і того ж сеансу, для надійності, можна передавати кількома транспортними сполученнями. Керує цими процесами *відображення сеансового сполучення на транспортне*.

За допомогою функції *закінчення сеансового сполучення* можна так закінчити сполучення, щоб рівень відображень не втратив жодного блоку, який ще перебуває в дорозі.

Транспортний рівень надає прикладним об'єктам сполучення через усі фізичні засоби мережі, незалежно від реальної конфігурації цього сполучення. Таке сполучення називають *наскрізним*. Сполучення, гарантоване транспортним рівнем, повинно бути *прозорим*, тобто не залежати від кодів інформації вищих рівнів. Для ефективнішого передавання даних на транспортному рівні є кілька класів сервісу, які відрізняються параметрами – перепускною здатністю, часом передавання, часом налагодження сполучення, допустимою ймовірністю помилок. Сервіс транспортного рівня передбачає такі функції:

- налагодження та розірвання транспортного сполучення;
- керування послідовністю блоків;
- забезпечення цілісності даних;
- зчеплення блоків та сегментування;

- виявлення та виправлення помилок;
- вибір класу сервісу;
- передавання даних;
- мультиплексування та розщеплення сполучень.

Транспортний рівень не тільки дає змогу вибрати певний клас сервісу, а й поновлює блоки даних, втрачені на першому–третьому рівнях. У випадку відмови сполучення на мережевому рівні він налагоджує інше мережеве сполучення. Транспортний рівень виконує мультиплексування та розщеплення сполучень, пріоритетне передавання блоків, оптимізує параметри передавання.

Функціонування транспортного рівня передбачає три фази, що змінюють одна одну:

- налагодження транспортного сполучення: вибір класу сервісу, прийняття рішення про потребу мультиплексування, визначення оптимального розміру блоку даних;
- передавання даних: організація послідовності блоків даних, сегментування блоків, мультиплексування та розщеплення сполучень, виявлення та виправлення помилок;
- завершення сполучення.

Мережевий рівень виконує ретрансляцію даних через одну або кілька систем, а також забезпечує для транспортного рівня незалежність від методів та засобів комутації, різних маршрутів у фізичних засобах сполучення. На цьому рівні реалізується маршрутизація інформації, тобто вибираються шляхи передавання блоків залежно від адрес призначення та інших характеристик (таких, як завантаженість або надійність окремих проміжних сполучень). Протокольні блоки даних на мережевому рівні називають **пакетами** (packets).

Головні різновиди сервісу мережевого рівня:

- організація мережевих сполучень;
- ідентифікація кінцевих точок сполучення;
- передавання блоків даних;
- керування потоками блоків даних;
- виявлення помилок;
- ліквідація мережевих сполучень.

Канальний рівень призначений для передавання блоків даних через одне фізичне сполучення. Тому на мережевому рівні типи фізичних сполучень, які розміщені нижче, не відомі.

Види сервісу канального рівня:

- передавання блоків даних;
- організація послідовності блоків;
- виявлення та виправлення помилок;
- керування потоком;
- налагодження та розірвання канальних сполучень.

Протокольні блоки даних канального рівня називають **кадрами** (frames). Важливою функцією, яку можна виконувати на канальному рівні, є *селекція інформації* – відбір серед всіх прийнятих блоків тільки тих, які адресовані конкретній системі.

Фізичний рівень призначений для спряження систем з фізичним середовищем. Він визначає механічні, електричні, функціональні та процедурні характеристики, які описують

доступ до фізичних сполучень. Фізичне сполучення забезпечує *прозорість*, тобто передавання довільної послідовності бітів. Через одне фізичне сполучення інформацію можуть передавати кілька канальних об'єктів або одне канальне сполучення можуть обслуговувати кілька фізичних. Є такі два типи фізичних сполучень для передавання даних:

- **двопунктове** (point-to-point connection) – це сполучення між двома станціями (рис.2.7);
- **багатопунктове** (multipoint connection) – між трьома і більше станціями (рис. 2.8).

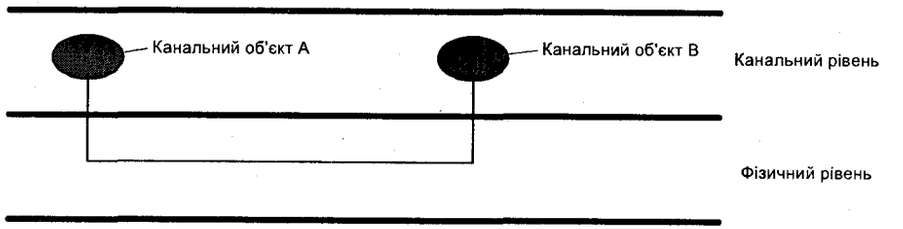


Рис. 2.7. Двопунктове сполучення.

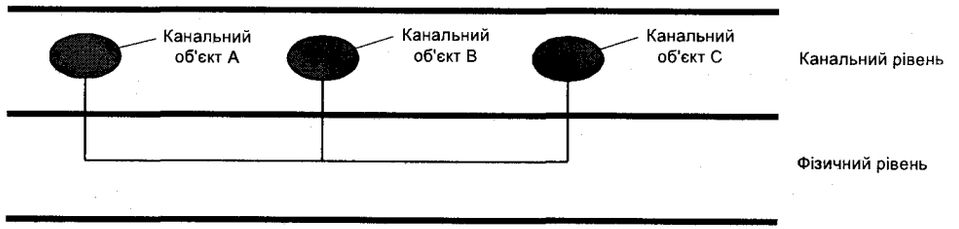


Рис. 2.8. Багатопунктове сполучення.

Фізичний рівень забезпечує такі різновиди сервісу:

- налаштування постійних або тимчасових фізичних сполучень;
- ідентифікація фізичних сполучень;
- організація послідовного передавання;
- повідомлення про розриви, збої.

На фізичному рівні відбувається прослуховування багатопунктового сполучення для визначення наявності передавання, зіткнення кадрів та ін.

2.4. Методи комутації

У розділі 1 (див. рис. 1.3) комунікаційна мережа описана сукупністю вузлів та каналів зв'язку, що їх сполучають. Вузли мережі забезпечують опрацювання та збереження даних, а також їхню комутацію. Канали зв'язку реалізують передавання даних. Два або більше комп'ютерів можуть бути сполучені каналами зв'язку по-різному.

Спосіб сполучення комп'ютерів каналами зв'язку для передавання даних між ними називається ***методом комутації****.*

Різні методи комутації можна систематизувати так, як це показано на рис. 2.9.

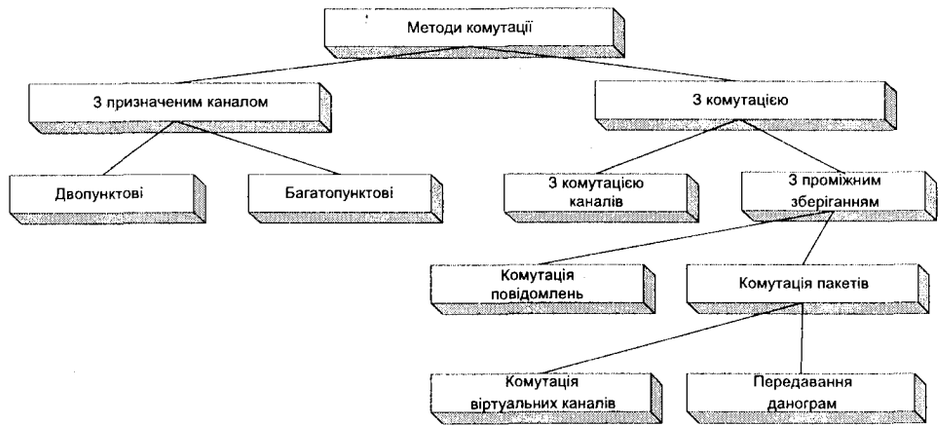


Рис. 2.9. Класифікація методів комутації.

Комутація з використанням **призначених каналів зв'язку**. У цьому випадку між комп'ютерами налаштовують постійно діючий канал зв'язку з фіксованою швидкістю передавання даних та смугою перепускання. Налаштування та підтримка такого каналу, особливо на далеку відстань, коштує дорого. Крім того, якщо навантаження невелике або нерівномірне, перепускна здатність каналу зв'язку використовується неефективно. Призначені канали можна встановити за *дво-* або *багатопунктовою* схемою.

- **Двопунктове** – це сполучення призначеним каналом двох комп'ютерів. Його використовують як у локальних, так і в глобальних КМ для передавання великих обсягів даних.
- **Багатопунктове** – це сполучення трьох або більше комп'ютерів призначеним каналом. Сам канал у цьому випадку експлуатується в режимі розподілу. Ефективність його використання більша ніж двопунктового. Багатопунктове сполучення застосовують тільки в локальних КМ, воно потребує спеціальних засобів керування розподілом каналу.

У сполученнях **з комутацією**, на відміну від методу з призначеним каналом, зв'язок між комп'ютерами є не постійний, а відбувається за запитом. Ці методи комутації поділяють на дві групи: *з комутацією каналів* та *з проміжним зберіганням*.

• У випадку **комутації каналів** за запитом одного з учасників обміну між двома комп'ютерами налаштовується канал зв'язку. Він може складатися з багатьох ланок. Якщо одна з ланок зайнята, канал не налаштовується. Коли канал налаштовано, він має фіксовану смугу перепускання та швидкість передавання. Після завершення передавання відбувається роз'єднання, канал руйнується. Прикладом комутації каналів можна вважати роботу телефонної мережі. Недоліками цього методу є тривалий час налагодження сполучень, неефективність використання каналу зв'язку, якщо навантаження мале та нерівномірне. Низька якість телефонних каналів та зумовлене цим зменшення вислідної швидкості передавання знижують ефективність використання каналу зв'язку ще більше. Сьогодні комутацію каналів у КМ використовують там, де треба передавати дані через модем і телефонну мережу (непризначеними каналами). Це потрібно під час роботи користувача з більшістю глобальних мереж (Internet, Relcom, Compuserve), а також для організації віддаленого доступу в локальну або корпоративну мережу через модем. Водночас принципи комутації є в основі найперспективніших технологій передавання інформації (ATM) і сфера їх застосування у швидкісних мережах постійно збільшується.

• Під час передавання даних **з проміжним зберіганням** інформація затримується, накопичується та аналізується в проміжних вузлах передавання. Це зумовлює потребу мати у вузлах буфери достатніх розмірів для запам'ятовування інформації, процесори для її опрацювання. Щоб уникнути переповнення буферів, треба реалізувати механізми керування потоком. У цілому методи комутації з проміжним зберіганням дають змогу досягти більшої ефективності використання каналів зв'язку завдяки їхній гнучкості. Серед методів з проміжним зберіганням розрізняють *комутацію повідомлень* та *комутацію пакетів*.

• У **комутації повідомлень** під повідомленнями розуміють інформаційний об'єкт, який треба передати: файл, зображення тощо. Таке повідомлення передається, як одне ціле. Оскільки повідомлення можуть мати великий обсяг, то використання такої техніки комутації потребує великих буферів (на максимальний обсяг повідомлення), тривалих затримок передавання (доки не буде прийняте все повідомлення в проміжному вузлі, подальше передавання блоковане). Усе це зумовлює неефективність використання каналу. Тому метод комутації повідомлень на практиці застосовують зрідка.

• У методі **комутації пакетів** усе повідомлення поділяється на пакети фіксованої довжини. Кожен пакет передається незалежно від інших. Такий метод дуже гнучкий, оскільки не потрібно чекати на приймання повного повідомлення в проміжних вузлах, у випадку спотворення якогось пакета не треба повторювати передавання інших пакетів. Одним каналом зв'язку можна одночасно передавати пакети з різних повідомлень різних абонентів мережі, що підвищує ефективність використання каналу. Методи комутації пакетів сьогодні найпоширеніші в КМ. Серед них можна виділити *метод комутації віртуальних каналів* та метод *передавання даннограм*.

• Метод **комутації віртуальних каналів** полягає в тому, що перед початком сполучення в мережу надсилається спеціальний пакет, який, проходячи нею, налаштовує з окремих її ланок *віртуальний канал*. Отже, віртуальний канал – це послідовність ланок передавання, що веде від відправника до одержувача. Кожному віртуальному каналу присвоюється унікальний номер. У кожен момент часу в мережі не може бути двох віртуальних каналів з однаковими номерами. Після налагодження віртуального каналу пакети повідомлення надходять визначеним каналом. З адресної інформації такі пакети містять тільки номер віртуального каналу. Після закінчення передавання віртуальний канал розпадається. Канал називається *віртуальним* тому, що, на відміну від призначеного або комутованого, реальний канал, який використовує конкретний віртуальний канал, може передавати водночас пакети кількох віртуальних каналів. Це підвищує ефективність використання каналу. Метод комутації віртуальних каналів дає змогу зменшити службову адресну інформацію на 8–10% порівняно з методом даннограм. Крім того, операції аналізу пакета в кожному вузлі (і відповідна затримка) максимально спрощені – аналізується тільки номер каналу.

• У випадку передавання **даннограм** повідомлення поділяють на окремі незалежні пакети – даннограми. Кожна даннограма обов'язково містить адреси відправника та одержувача. Даннограми нумерують та передають незалежно одну від одної. Одержувач формує повідомлення з даннограм. Даннограми потребують більшого аналізу в проміжних вузлах передавання, ніж пакети віртуальних каналів. З іншого боку, даннограми одного повідомлення не прив'язані до якогось визначеного маршруту в мережі. Їх можна передавати різними маршрутами одночасно, зменшуючи тривалість передавання всього повідомлення.

Порівняємо вартість та сфери застосування різних методів комутації. На рис. 2.10 зображено якісний графік залежності вартості передавання даних від обсягу інформації, що передається, для трьох різних методів комутації. Зроблено припущення, що відстань передавання та смуга перепускання – сталі.

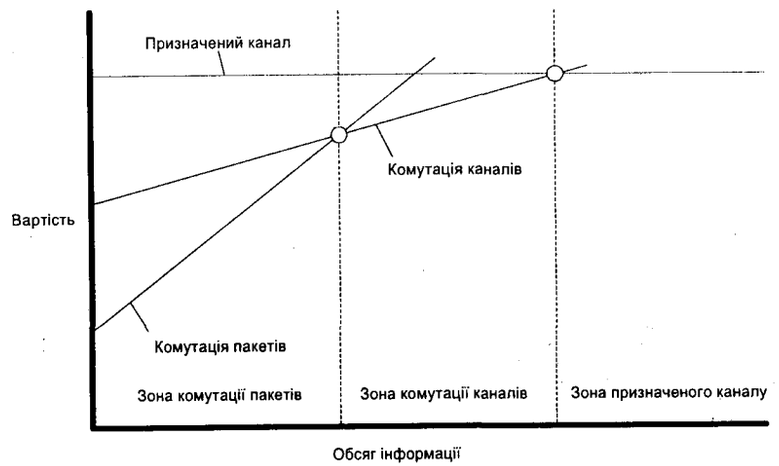


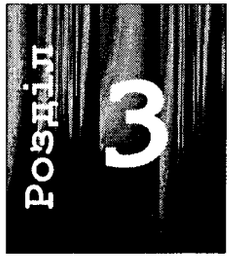
Рис. 2.10. Сфери застосування різних методів комутації.

Для призначеного каналу вартість не залежить від обсягу інформації, якщо перепускна здатність каналу фіксована. Для комутації каналів значну вартість має початкове налаштування каналу. Вона також збільшується зі збільшенням обсягу переданої інформації. У комутації пакетів початкові затрати менші, ніж у випадку комутації каналів. Однак зі збільшенням навантаження затрати збільшуються стрімкіше, оскільки потрібні ресурси для опрацювання пакетів у проміжних вузлах. Отже, на графіку можна виділити три сфери застосування різних методів комутації. Якщо навантаження невеликі (щодо максимальної пропускної здатності), то ефективним є використання комутації пакетів. Для середніх навантажень ефективна комутація каналів, а для великих та постійних – призначений канал.

Бібліографія та джерела

1. Архитектура, протоколы и тестирование открытых информационных сетей: Толковый словарь / Под ред. Э.А. Якубайтиса. М.: Финансы и статистика, 1989.
2. *Вейцман К.* Распределенные системы мини и микро ЭВМ / Пер. с англ. М.: Финансы и статистика, 1982.
3. *Коссак О.М.* Англо-український словник з інформатики та обчислювальної техніки. Львів: БаК, 1995.
4. *Коссак О., Кравець Р.* Англо-український та українсько-англійський словник-довідник з телекомунікацій. Львів: БаК, 1996.
5. *Мизин И.А., Богатырев В.А., Кулешов А.П.* Сети коммутации пакетов. М.: Радио и связь, 1986.

СЕРЕДОВИЩА ПЕРЕДАВАННЯ ДАНИХ, СИГНАЛИ ТА КОДИ КОМП'ЮТЕРНИХ МЕРЕЖ



Середовища передавання в комп'ютерних мережах. Техніко-експлуатаційні характеристики. Ефірні середовища. Коаксіальні кабелі. Волоконно-оптичний кабель. Скручена пара. Сертифікація кабелів. Структурна схема ланки передавання. Кодування та модуляція. Характеристика завад у каналі зв'язку. Форми передавання даних у КМ. Синхронне та асинхронне передавання.

3.1. Середовища передавання у комп'ютерних мережах

Техніко-експлуатаційні характеристики середовищ передавання такі: час і швидкість розповсюдження сигналів, вартість, швидкість загасання сигналу на одиницю довжини кабелю з урахуванням його частоти, опір одного метра, маса одного метра, завадостійкість у різних навколишніх середовищах, випромінювання в довкілля.

Важливим параметром якості кабелю є ***перехідне загасання на ближньому кінці*** *(Near End Crosstalk (NEXT)). Електричний струм у дроті створює електромагнітне поле, яке відповідно спричинює завади в сусідніх дротах, причому чим більша частота сигналу, тим більші завади. NEXT характеризує ступінь цих завад. У якісних кабелях з високим загасанням рівень корисного сигналу значно вищий, ніж рівень завад, які генеруються в цьому випадку.*

Параметр ***випромінювання в довкілля*** *(Electromagnetic Interference (EMI)) характеризує ступінь та параметри паразитного випромінювання, яке генерується під час передавання сигналу кабелем (див. Додатки до розділу 3.*

У КМ можна використовувати такі середовища передавання.

Ефірні середовища

Передавання в ефірних середовищах відбувається без використання кабелів. Залежно від частоти передавання ефірні канали поділяють на радіо-, інфрачервоні, ультракороткохвильові, мікрохвильові.

Будь-який **радіоканал** формується на певній частоті-носію. Інформація по ньому передається за допомогою модульованого радіосигналу. Канал характеризується невисокою швидкістю передавання (20–150 Кбіт/с), середньою вартістю, доступністю для всіх видів радіозавад, працює тільки в межах радіодосяжності. Його використовують головно в пересувних станціях.

В **інфрачервоному каналі** сигнали інфрачервоних частот передають малогабаритні передавачі та приймають чутливі приймачі. Канал працює тільки в межах прямої оптичної

видимості. Він нечутливий до електромагнітних завад. Відстань між станціями – до 3 км, швидкість передавання – 2–4 Мбіт/с. Приймачі та передавачі інфрачервоного діапазону досить дешеві. Недоліки каналу: недовговічність апаратури, велике загасання сигналів, якщо погана прозорість повітря (наприклад, є запиленість).

Для налагодження **ультракороткохвильового каналу** потрібна ультракороткохвильова приймальна та передавальна апаратура. Передавання відбувається за допомогою частотно-модульованих сигналів у досить широкому діапазоні частот. Це дає змогу створити велику кількість каналів. Інформація передається на відстань 0.7–1.5 км зі швидкістю 20–40 Мбіт/с. Переваги каналу такі: мала потужність апаратури, наявність великої кількості каналів, можливість роботи в умовах поганої та непрямої видимості. Загалом ультракороткохвильовий канал має таку ж ефективність, як і радіоканал.

У **мікрохвильовому каналі** використано нову форму середовища передавання даних. Сигнали випромінюють спеціальні лазери, а приймають фотозчитувачі. Канал добре працює в зоні прямої видимості. Інформація передається на відстань 15–20 км зі швидкістю до 20 Гбіт/с. Апаратура каналоутворення сьогодні є досить дорогою і недостатньо досконалою.

Загалом ефірними середовищами передається до кількох відсотків загального обсягу інформації КМ. Сьогодні значення таких середовищ у КМ зростає, що пов'язане з розвитком мереж безпроводового передавання (див. розділ 26).

Коаксіальний кабель

Коаксіальні кабелі поряд зі скрученою парою є найпоширенішим середовищем передавання даних у КМ. Вони мають високу швидкість передавання, завадостійкість, довговічність, помірну вартість. Для них розроблені прості засоби спряження з ЛМ.

За техніко-експлуатаційними характеристиками розрізняють широко- та вузькосмугові коаксіальні кабелі.

Широкосмугові коаксіальні кабелі мають швидкість передавання сигналу 300–500 Мбіт/с, загасання сигналу на частоті 100 МГц – до 7 Дб на 100 м. Термін придатності – 10–12 років. Погонна затримка поширення сигналів – 2–5 нс/м.

Вузькосмугові кабелі мають швидкість передавання до 50 Мбіт/с, загасання сигналів на частоті 10 МГц – 4 Дб на 100 м. Решта параметрів збігається з аналогічними в широкосмугових кабелях.

Довжина кабелю в КМ переважно визначається загасанням сигналу. Якщо сигнал загасає дуже сильно, то ставлять повторювач, який поновлює його.

Волоконно-оптичний кабель

У цих кабелях як фізичне середовище використовують прозоре скловолокно. Найпростіший кабель складається з кварцової серцевини діаметром 20–60 мкм, навколо якої нанесена тонка плівка з меншим коефіцієнтом відбиття. Швидкість передавання сигналів кабелем 0.2–1.0 Гбіт/с. Теоретично можлива максимальна швидкість передавання – 200 Гбіт/с. Довжина сполучень – 110 км.

*Розрізняють два типи оптичних волокон: одно- та багатомодові. В **одномодових** волокнах серцевина має діаметр ≈ 10 мкм. Для генерації світла використовують напівпровідникові лазери. Передавання інформації відбувається на довжинах хвиль 1.3, 1.55 мкм. Смуга перепускання – 2 ГГц, її ширина не залежить від довжини лінії. Загасання сигналу 0.7 Дб/км. У кожен момент часу може поширюватись сигнал тільки одного променя (моди). Максимальна відстань передавання – до 110 км. Однак вартість лазерів та фотоприймачів висока.*

*У **багатомодових** волокнах діаметр серцевини ≈ 50.0, 62.5, 100.0, 140.0 мкм. Для генерації світла використовують суперлюмінесцентні діоди. Передавання інформації відбувається на хвилях 1.3 та 0.85 мкм. Смуга перепускання – 800–900 МГц, її ширина залежить від довжини лінії. Загасання сигналу 0.5–7.0 Дб/км. Максимальна відстань передавання – кілька кілометрів. Одночасно можуть передаватися сигнали кількох променів (мод), що входять у кабель під різними кутами.*

У волоконно-оптичних кабелях значно менше (порівняно з коаксіальними) загасання сигналів, вища швидкість передавання, широка частотна смуга передавання, вони нечутливі до електромагнітних завад. Водночас такі кабелі мають малу механічну стійкість, їх не можна гнути, терти, пересувати, вони не витримують вібрації. Якщо виник розрив, то його треба заварити, для чого потрібне складне та дороге обладнання. Крім того, в місці зварювання буде втрачатися частина сигналу. Це стримує їхнє розповсюдження. Сьогодні волоконно-оптичні кабелі вважають найперспективнішими для нової АТМ технології передавання даних, побудови магістральних інформаційних мереж.

Спочатку волоконно-оптичні кабелі виготовляли зі скла. Сьогодні щораз частіше застосовують прозорі пластикові волокна. Це значно підвищує механічну стійкість, однак зменшує допустиму відстань передавання.

Скручена пара дротів

Цей тип кабелю є найдешевшим і найпоширенішим. Максимальна відстань передавання у ньому 1.5–2.0 км, максимальна швидкість – 1.2 Гбіт/с. Має гірший, ніж у коаксіальному кабелі, захист від завад. Тривалість поширення сигналу 8–12 нс/м. Загасання сигналу 12–28 Дб на 100 м на частоті 10 МГц. Термін експлуатації – 2–6 років. Канал найдешевший в укладанні. Сьогодні скручена пара є головним середовищем передавання в локальних мережах.

Розрізняють декілька типів скручених пар. Найрозповсюдженішою є **неекранована** (Unshielded Twisted Pair (**UTP**)). Вона найдешевша, однак під час її експлуатації виникають проблеми з EMI. Крім того, використовують **фольговану** (Folged Twisted Pair (**FTP**)), та **екрановану** скручені пари (Shielded Twisted Pair (**STP**)), а також їхні комбінації.

Плаский кабель

Такий кабель складається з 12 і менше дротів, об'єднаних загальною екранною сіткою та ізольованих один від одного. Передавання відбувається на відстань до 15 м. Швидкість передавання така ж, як у скрученої пари.

3.2. Сертифікація кабелів комп'ютерних мереж

Сертифікацією кабелів займаються **IEEE, EIA/TIA** (Electronic Industry Association/ Telecommunication Industry Association), а в США – фірма **UL** (Underwriter Laboratories – Лабораторії сертифікації). Кабелі сертифікують щодо електричної безпеки (відповідно до вимог стандартів National Electric Code (**NEC**)) та за технічними характеристиками (відповідно до вимог EIA/TIA). Тільки після сертифікації фірма-виробник кабелю може поставити на ньому знак UL. З метою дотримання якості продукції UL проводить інспекції виробництва, де, крім готової продукції, контролює також окремі технологічні процеси.

Залежно від ступеня електробезпеки в КМ бувають кабелі зв'язку та слабкострумові кабелі. За технічними параметрами кабелі UTP поділяють на класи, або категорії. Розрізняють сім категорій кабелю (табл.3.1). Детальна специфікація технічних вимог до кабелів різних категорій є в стандартах EIA/TIA 568, ISO 11801, EN 50173.

Таблиця 3.1. Категорії та класи кабелів

Частота, МГц	Швидкість передавання, Мбіт/с	Клас, категорія	Використання	Примітка
< 1	до 20 Кбіт/с	1, A	Передавання даних та мовлення	Параметри не специфікуються
1	1	2, B	ISDN	
16	16	3, C	LAN	
20	20	4	ED LAN	
100	100	5, D	HS LAN	
100	1000	5+	Gigabit Ethernet	
200	> 1 Гбіт/с	6, E		
600		7, F		

3.3. Структурна схема ланки передавання даних

Сукупність засобів фізичного та канального рівнів утворює певну систему, що називається **ланкою, або каналом передавання даних** (рис. 3.1). Канал передавання даних складається з таких елементів:

- фізичного середовища передавання та відповідних роз'єднувачів (фізичного каналу);
- засобів перетворення цифрових даних, які виробляє комп'ютер, у форму, прийнятну для передавання фізичним каналом (сигнал даних) та навпаки. Такі засоби називаються **пристроями спряження** (Media Access Unit (**MAU**));
- засобів керування ланкою даних.

Конкретніше каналом передавання даних називають сукупність програмно-технічних засобів та фізичного середовища передавання, призначених для передавання сигналу даних.

*З погляду користувача головна характеристика каналу зв'язку – кількісні та якісні параметри сервісу, які надає його продавець. Сьогодні визначено багато загальноприйнятих типів каналів. Наприклад, служба **Switched 56** – це канал з перепускною здатністю 56 Кбіт/с. Канал Т1 – має перепускну здатність 1.544 Мбіт/с, а канал Т3 – 45 Мбіт/с. Каналам Т1, Т3, які діють у США, у Європі відповідають канали Е1 та Е3 з перепускною здатністю 2.048 та 34.368 Мбіт/с. Залежно від перепускної здатності канали утворюють ієрархії. Традиційні телефонні ІКМ-канали мають **плезіохронну ієрархію**. Перепускна здатність волоконно-оптичних каналів зумовлює **синхронну ієрархію** (див. Д.3.2).*

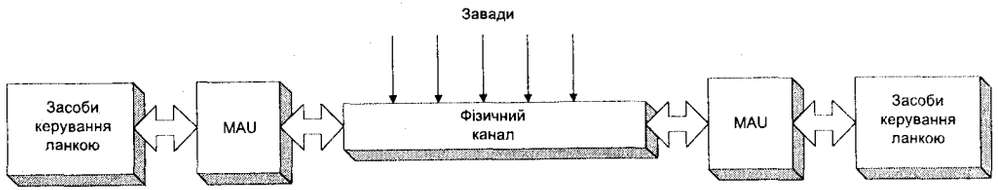


Рис. 3.1. Структура ланки передавання даних.

За напрямками розрізняють такі передавання даних у каналі зв'язку:

- **симплексне** (simplex) – передавання в одному напрямі;
- **напівдуплексне** (duplex) – передавання по черзі в прямому та зворотному напрямах;
- **дуплексне** (full duplex) – передавання одночасно в прямому та зворотному напрямах.

Пристрій спряження MAU виконує дві головні функції: *кодування (декодування)* та *модуляцію (демодуляцію)*.

Кодування – це певне перетворення цифрового коду, що надходить від комп'ютера, з метою збільшити його завадостійкість та для зручності передавання.

Модуляцією називають процес переходу від кодового сигналу до сигналу даних.

Як звичайно, для цього використовують сигнал-носій, деякі параметри якого змінюються відповідно до зміни кодового сигналу. У системах зв'язку найпоширеніші модуляція гармонічних коливань та імпульсна модуляція.

У випадку модуляції гармонічних коливань носіями є гармонічні коливання струму або напруги. Залежно від того, який параметр гармонічного коливання змінюється, розрізняють амплітудну, фазову та частотну модуляції. У комп'ютерних мережах переважно використовують фазову або частотну модуляції. Амплітудну модуляцію, порівняно з іншими, більше спотворюють завади. (Загасання сигналу призводить до зменшення його амплітуди).

В імпульсній модуляції носієм є послідовність імпульсів. Залежно від параметрів цієї послідовності, які змінюються відповідно до кодового сигналу, розрізняють амплітудно-імпульсну, широтно-імпульсну, фазово-імпульсну та частотно-імпульсну модуляції. Для передавання даних магістральними телефонними каналами найчастіше застосовують імпульсно-кодову модуляцію (ІКМ) (див. Д.3.3).

Для передавання даних в аналоговій формі у глобальних мережах (найчастіше телефонним каналом) використовують модеми, у локальних – спеціальні адаптери, які значно збільшують швидкість передавання і можуть передавати дані як в аналоговій, так і цифровій формах, а також лінійні контролери, які передають дані в цифровій формі.

На фізичний канал передавання даних впливають завади, які спотворюють сигнал та призводять до виникнення помилок. З впливом завад борються на фізичному та канальному рівнях протоколу, в тому числі засобами керування каналом передавання даних.

3.4. Характеристика завад у каналі зв'язку

Розглянемо вплив завад на сигнал, який передається у фізичному каналі, детальніше. Якщо на вході фізичного каналу маємо сигнал $z(t)$, то на виході унаслідок впливу завад – спотворений сигнал $z'(t)$. Якщо $z'(t)$ та $z(t)$ пов'язані певною функціональною залежністю, яка дає змогу повністю поновити початковий сигнал, то відповідна завада називається *регулярною*. За впливом на вхідний сигнал завади $\xi(t)$ поділяють на *адитивні* $\xi_a(t)$ та *мультиплікативні* $\xi_m(t)$. Для адитивної завади залежність між сигналом на виході каналу та сигналом на вході можна записати у вигляді суми

$$z'(t) = z(t) + \xi_a(t).$$

Для мультиплікативних завад цю залежність описує рівняння

$$z'(t) = z(t)\xi_m(t).$$

Якщо характеризувати завади зі статистичного погляду, то їх можна розділити на флуктуаційні та імпульсні. *Флуктуаційні* завади описує неперервна випадкова функція часу. Такі завади формуються як накладання великої кількості різних завад з різних джерел. Як звичайно, серед цих складових нема окремих імпульсів, які б перевищували загальний рівень сигналу у три-чотири рази і більше. *Імпульсні* завади – це послідовність імпульсів з випадковими амплітудами, шириною та часом появи. Серед таких завад найбільшу небезпеку створюють імпульси, амплітуда яких наближена до величини сигналу, що передається.

3.5. Форми передавання даних у каналах КМ

Цифрові дані в КМ передаються послідовно, тобто бітами, що суттєво відрізняється від передавання даних між пристроями однієї ЕОМ, де воно відбувається паралельно. Фізично біти передаються у формі сигналів. Є два головні типи сигналів – *аналогові* та *цифрові*. Під час роботи з аналоговими сигналами використовують модульований сигнал синусоїдної форми, а для роботи з цифровими – дворівневий дискретний сигнал (рис.3.3). Аналогові сигнали менш чутливі до спотворень та загасання, але потребують апаратури для модуляції та демодуляції.

Менша завадостійкість цифрового сигналу призводить до того, що цифрове передавання між терміналом та комп'ютером обмежується відстанню 20–300 м залежно від типу кабелю (конденсаторний ефект, вплив погонної індуктивності).

З типом передавання сигналу тісно пов'язані поняття вузько- та широкосмугового передавання.

Вузькосмугове передавання *(baseband) є цифровим. У цьому випадку передавання та приймання відбуваються одночасно, використовується вся смуга перепускання кабелю. Для підсилення сигналу такого передавання застосовують* ***повторювачі*** *(repeaters).*

Широкосмугове передавання *(broadband) є аналоговим. Смуга перепускання каналу поділена на окремі діапазони частот, що їх використовують різні канали. Для поновлення сигналу застосовують* ***підсилювачі*** *(amplifiers).*

Форми зображення та загасання аналогового та цифрового сигналів показані на рис.3.2.

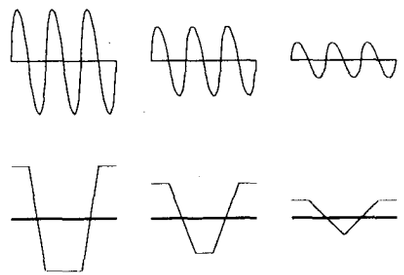


Рис. 3.2. Спотворення аналогового та цифрового сигналів у випадку загасання.

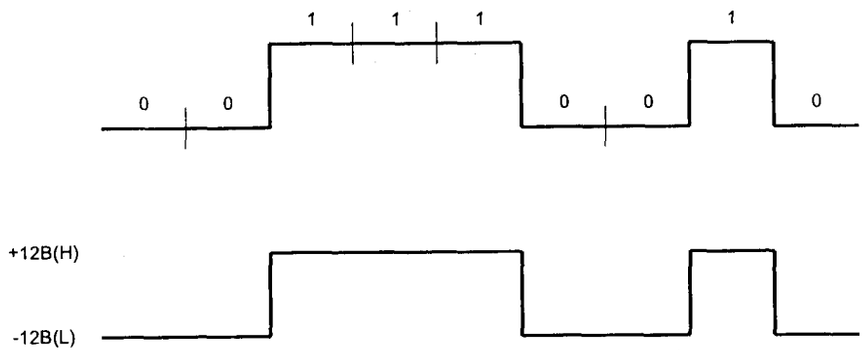


Рис. 3.3. Цифрові дані в формі NRZ.

Передавання цифрових даних відбувається без модуляції. У цьому випадку використовують метод за формою сигналу **без повернення до нуля** (Non Return to Zero (**NRZ**)) (рис. 3.3).

Як видно з рис. 3.3, визначити, де починаються і закінчуються логічні 0 та 1, важко. Для розпізнавання моментів закінчення та початку логічних сигналів використовують синхронізацію.

3.6. Синхронізація

Проблему синхронізації можна вирішити кількома способами. Один з них полягає у виділенні спеціальної лінії, якою передається сигнал тактової частоти – *синхросигнал*. У скрученій парі або коаксіальному кабелі такою лінією є другий дріт. У цьому випадку передавання називається синхронним (рис. 3.4).

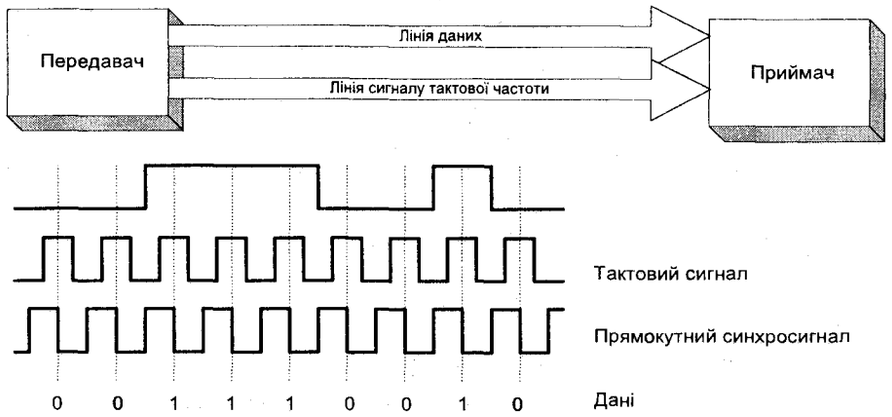


Рис. 3.4. Синхронне передавання.

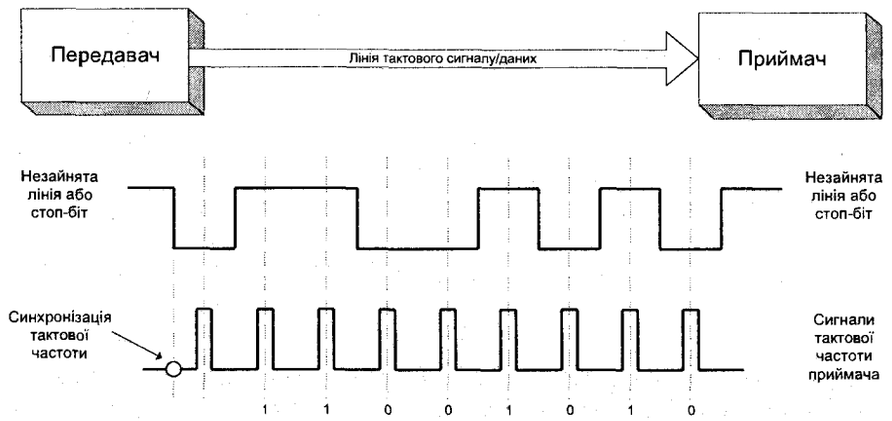


Рис. 3.5. Асинхронне передавання.

Синхронним передавання може бути і без окремої лінії. У цьому випадку синхросигнал передається разом із даними, а також у проміжках між їх передаванням. Якщо ж у проміжках між передаванням даних синхросигнал не передається, то таке передавання називається **асинхронним** або **з автоналагоджуванням**. При низьких швидкостях ефективніщим є асинхронне передавання, при високих – з автоналагоджуванням або синхронне.

У випадку асинхронного передавання потік бітів ділиться на байти. Приймач та передавач мають вбудовані тактові генератори з однаковими частотами (допускається така похибка, яка унеможливлює розходження частот генераторів під час передавання одного байта на значення, що призведе до помилки в результатах). Перед кожним байтом передається стоп-біт. Він також передається, якщо канал вільний. Під час переходу з високого рівня на низький генератор налагоджується, пропускає один біт і приймає один байт (рис. 3.5).

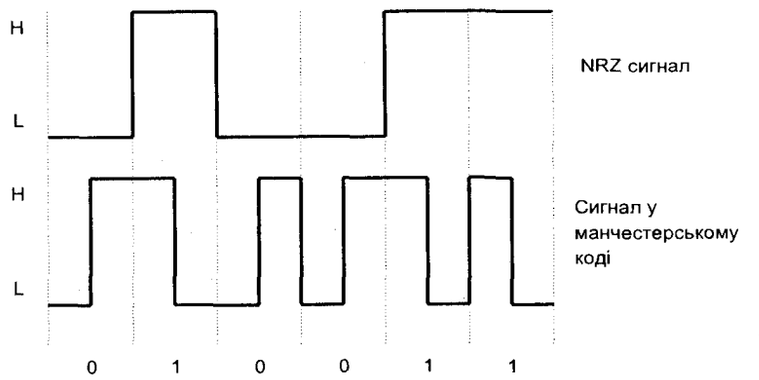


Рис. 3.6. Манчестерське кодування.

Прикладом передавання з автоналагоджуванням є манчестерське кодування (рис. 3.6). Його використовують у ЛМ Ethernet. Тактовий генератор приймача синхронізується під час передавання кожного біта у випадку переходу з H в L у середині інтервалу біта. Передавати можна необмежені послідовності бітів. Якщо інформація не передається, то генератори передавача та приймача розладнані. Тому перед передаванням треба надіслати спеціальну послідовність бітів – *преамбулу* – для синхронізації передавача і приймача, наприклад, 11111110.

3.7. Пристрій спряження

Усі внутрішні машинні операції виконуються з використанням цифрових сигналів паралельно. Як уже зазначалося, перетворює цифрові сигнали у форму, сприйнятну для передавання в КМ та навпаки, пристрій спряження (рис. 3.7).

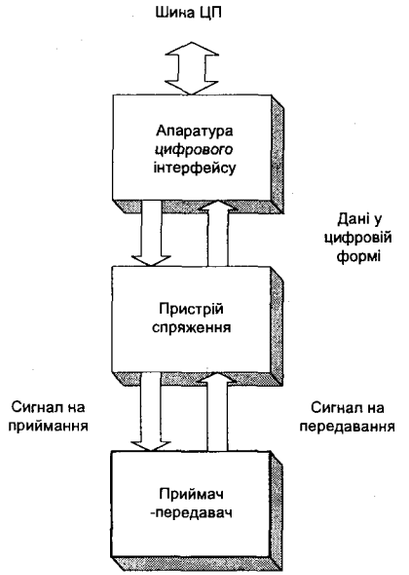


Рис. 3.7. Пристрій спряження в КМ.

Діаграма, на прикладі якої можна пояснити роботу пристрою спряження для середовища, яке використовує манчестерський код та аналоговий сигнал з амплітудною модуляцією, показана на рис. 3.8.

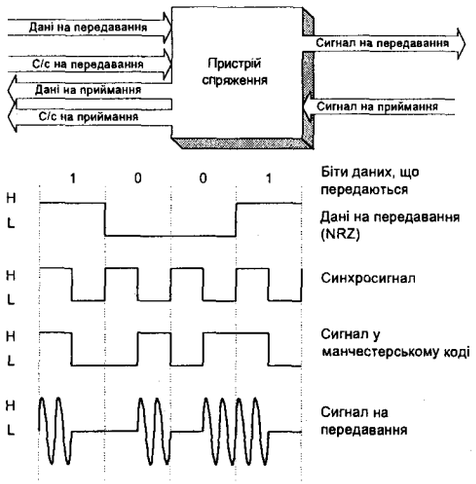


Рис. 3.8. Перетворення сигналів під час передавання даних у MAU.

Бібліографія та джерела

1. *Бараш Л.* Быстрые байты в телефонной сети // Комп'ютерное обозрение. 1998. №5 (124).
2. *Гальперович Д.* Расширенная категория 5 или категория 6 // LAN. 1998. № 4.
3. *Кларк Э.* Высокоскоростные кабели в действии // LAN. 1998. № 4.
4. Локальные вычислительные сети. Принципы построения, архитектура, коммуникационные средства / Под ред. С.В.Назарова. М.: Финансы и статистика, 1994.
5. Локальные вычислительные сети. Технические и программные средства / Под ред. С.В.Назарова. М.: Финансы и статистика, 1994.
6. *Овчинников В.В., Рыбкин И.И.* Техническая база интерфейсов локальных вычислительных сетей. М.: Радио и связь, 1989.
7. *Прангишвили И.В.* Микропроцессоры и локальные сети микро-ЭВМ в распределенных системах управления. М.: Энергоатомиздат, 1985.
8. *Прошин Д.* SDH: помнишь, как все начиналось // Сети. 1997. № 7.
9. *Райс Л.* Эксперименты с локальными сетями микро-ЭВМ. М.: Мир, 1990.

ДОДАТКИ ДО РОЗДІЛУ 3

Д.3.1. Характеристики EMI для різних типів скрученої пари

Під час передавання даних у сучасних мережах на високих частотах суттєвим стає вплив EMI на довкілля. Значне випромінювання може призвести до спотворення даних, нестабільної роботи приладів, аварій, негативно впливати на здоров'я людей.

Передусім це стосується найпоширенішого сьогодні середовища передавання даних у локальних мережах – неекранованої скрученої пари. UTP складається з чотирьох пар мідного дроту в PVC ізоляції. Значення EMI повинне зменшуватися внаслідок того, що сигнали в кожному дроті пари мають протилежну полярність і компенсують випромінювання один одного. Ступінь компенсації називається *збалансованістю*. Однак під час експлуатації мереж виявилось, що будь-які зміни мережі чи близькість металевого об'єкта можуть порушити баланс. Крім того, збалансованість залежить ще й від довжини кабелю. Отже, ступінь EMI для UTP передбачити неможливо.

Комісія Європейської Спільноти (Commission of European Communities (**CEC**)) розробила єдиний європейський стандарт для електричного обладнання, якому повинні відповідати національні стандарти за EMI. Стандарт поширюється на всі мережі, встановлені після 1 січня 1996 року. Згідно з цим стандартом мережеве обладнання в промислових умовах повинно мати випромінювання до 40 Дб на відстані 10 м, для комерційних та непромислових умов експлуатації – до 30 Дб. Продукція, яка пройшла тестування на відповідність вимогам CEC, має позначку **CE** і допущена до використання та продажу в Європі. Діяльність мереж, які не відповідають стандарту за EMI, може бути припинена.

Ліпші показники EMI порівняно з UTP мають інші варіанти скрученої нари – FTP, STP та їхні комбінації SFTP, S/STP, F/STP. Порівняльні характеристики цих скручених пар наведені в табл. Д.3.1.

Таблиця Д.3.1. Порівняльні характеристики скручених пар

Показник	Назва				
	UTP	FTP	SFTP	S/STP	F/STP
Ціна USD за 1 км	200-300	280-420	460-690	700-1050	585-875
Максимальна частота, МГц	100	150	300	300	300
Товщина, мм	5.1	6.2	6.5	7.3	7
Встановлення	Легке	Легке	Легке	Важке	Важке
Заземлення	-	Важке	Легке	Легке	Важке

Д.3.2. Цифрові ієрархії

Магістральні канали з ІКМ утворюють *плезіохронну ієрархію*. В її основі є базовий канал на 64 Кбіт/с (Digital Signal level 0 (**DS0**)). Власне така перепускна здатність потрібна для передавання одного телефонного сигналу мовлення з використанням імпульсно-кодової модуляції. Наступний канал DS1 в американському варіанті ієрархії утворюють 24 канали DS0 + 8 біт/с. Перепускна здатність каналу DS1 1.544 Мбіт/с (T1). Загалом послідовність швидкостей американського варіанта плезіохронної ієрархії: 1.5, 6.0, 45.0, 150.0 Мбіт/с. У європейському варіанті ієрархії швидкостей канал E1 формують групуванням 32-х каналів DS0 і послідовність швидкостей така: 2, 8, 34, 150,... Мбіт/с (E1, E2, E3,...).

Для волоконно-оптичних каналів стандарт **SDH** (Synchronous Digital Hierarchy) був прийнятий у лютому 1988 р. комітетом T1X1 МККТТ (ITU). Доти синхронні оптичні системи у Європі та США розвивалися по-різному. Зокрема, у США великої популярності набув стандарт **SONET** (Synchronous Optical Network). Оскільки ж він не збігався з європейською ієрархією швидкостей телефонних каналів (різниця між E1 та T1), то у Європі підтримки не мав. Об'єднав європейську та американську системи стандарт SDH. Головні канали ієрархії SDH наведені у табл Д.3.2.

Табл. Д.3.2. Ієрархії SONET та SDN

Швидкість передавання, Мбіт/с	Рівень ієрархії SONET	Рівень ієрархії SDH
51.84	OC-1/STS-1	STM-0
155.52	OC-3/STS-3	STM-1
622.08	OC-12/STS-12	STM-4
2488.32	OC-48/STS-48	STM-16
9953.28	OC-192/STS-192	STM-64

Примітка. Головні скорочення: **STS** (Synchronous Transport Signal) – електричний сигнал; **OC** (Optical Carrier) – оптичний носій; **STM** (Synchronous Transport Mode) – режим синхронного передавання.

Д.3.3. Імпульсно-кодова модуляція

До появи цифрового передавання найпоширенішим було аналогове, наприклад, частотне стиснення. У цьому випадку кожний сигнал мовлення (діапазон 3.0–3.4 кГц) модулював свою власну частоту-носія (108, 104,..., 64 кГц). Потім ці сигнали зливалися в один, що змінювався у діапазоні 64–108 кГц. Окремі сигнали мовлення потім знову можна було виділити за допомогою спеціальних частотних фільтрів. Перевага аналогового передавання: воно менше спотворювало дані.

Імпульсно-кодову модуляцію розробив А.Х.Рівс ще у 30-ті роки. Весь процес перетворення сигналу характеризується трьома операціями: **дискретизацією, квантуванням, кодуванням**.

Спочатку для кожного сигналу мовлення з групи зчитується значення (відлік) у конкретний момент часу. Таким чином весь сигнал мовлення перетворюється у послідовність дискретних відліків (дискретизація).

Потім значенню кожного відліку ставлять у відповідність цифровий код. У цьому випадку подібні за значенням відліки заміняють однаковим кодом (квантування та кодування).

Набори кодових сигналів для відліків з певної групи первинних сигналів мовлення передаються як одне кодоване посилання (часове стиснення).

Переваги ІКМ:

- цифрове передавання дає змогу додатково захистити сигнал від спотворень завдяки завадостійкому кодуванню;
- цифрове передавання не потребує операцій демодуляції, цифрового опрацювання та модуляції під час проходження сигналом різноманітних комутаторів, а такі операції додатково спотворюють аналоговий сигнал;
- спрощує та здешевлює апаратуру;
- підвищує ефективність використання каналу зв'язку (завдяки стисненню).

ІКМ сьогодні – це основний метод модуляції у магістральних каналах телефонних мереж.

ПЕРЕДАВАННЯ ДАНИХ З ВИКОРИСТАННЯМ МОДЕМА

Способи організації передавання даних з використанням персонального комп'ютера. Стандарти RS-232C, RS-422, RS-423. Передавання даних з використанням нуль-модема. Модеми, їхня класифікація. Керування модемом. Передавання даних у двопроводовій лінії з використанням модема. Стандарти передавання даних.

4.1. Способи організації передавання даних з персонального комп'ютера

Розглянемо головні способи передавання даних з ПК. Можна виділити три принципово різні підходи до організації такого передавання:

- через послідовний порт, виконаний згідно зі стандартом RS-232C;
- через паралельний принтерний порт;
- з використанням спеціальної адаптерної плати, яку безпосередньо вмикають у роз'єднувач материнської плати комп'ютера і через нього приєднують до шини введення-виведення.

Передавання даних через послідовний порт відбувається з низькою швидкістю, проте апаратура послідовного порту є в кожному ПК, тому додаткові витрати на організацію передавання невеликі. Водночас застосування послідовного порту є єдиною можливістю організації передавання даних телефонною лінією з використанням модема.

Дані через паралельний порт передаються з більшою швидкістю, ніж через послідовний. Однак таким обміном користуються у випадку передавання на невелику відстань.

Передавання даних з використанням адаптерної плати має значно більшу швидкість, але й плата коштує дорого. Тому для епізодичних передавань, а також для приєднання модемів доцільно застосовувати послідовний порт. Адаптерні плати вигідно використовувати у справжній локальній мережі з постійним та оперативним доступом до даних.

4.2. Характеристика стандартів RS-232C, RS-422, RS-423

Стандарти інтерфейсів фізичного рівня для передавання на коротку відстань, приєднання терміналів, різних пристроїв тощо, становлять окрему групу.

*Ці стандарти класифікують як **інтерфейси**, окреслюючи цим той факт, що вони описують набір сигналів на **межі** між терміналом та комп'ютером, модемом та комп'ютером тощо.*

Найвідомішим з цієї групи є стандарт RS-232C. У ньому використано двопроводову лінію зв'язку, двополярні сигнали амплітудою 25 В. Стандарт розробляли в період рідкісного

використання інтегральних мікросхем. Максимальна швидкість передавання – 20000 біт/с, реальна швидкість залежить від відстані передавання.

Стандарт RS-232C був розроблений ще в 1969 р. Американською асоціацією електронної промисловості (American Electronics Industries Association (AEIA, або EIA)). Тому його інколи позначають EIA RS-232C. ITU розробив комплекс аналогічних стандартів V.24 (механічні характеристики) і V.28 (електричні характеристики), які функціонально відповідають EIA RS-232C.

У нових поліпшених стандартах RS-422, RS-423 враховано рівні сигналів інтегральних мікросхем, вони призначені для передавання даних на більші відстані і з більшою швидкістю.

Стандарт RS-422 регламентує роботу симетричної ланки зв'язку та використання коаксіальних кабелів. Передавання інформації виконується на відстань до 1220 м зі швидкістю до 10 Мбіт/с.

Стандарт RS-423 за можливостями посідає проміжне становище між RS-232C та RS-422. Він описує використання двопроводової, несиметричної лінії зв'язку. Максимальна довжина лінії 1220 м. Середня швидкість передавання 3 Кбіт/с. При максимальній швидкості 300 Кбіт/с довжина лінії не перевищує 12.2 м.

Незважаючи на те, що інтерфейси RS-423/422 мають ліпші характеристики передавання і планувалися для заміни RS-232C, вони не стали популярними. Детальніше стандарти RS-422, RS- 423, RS-449 схарактеризовані у Д.4.1.

4.3. Передавання даних з використанням нуль-модема та простих комунікаційних програм

Практично кожний ПК має апаратуру послідовного порту введення-виведення, виконаного відповідно до стандарту RS-232C. Тому розглянемо інтерфейс RS-232C детальніше.

Спочатку інтерфейс RS-232C був призначений для приєднання терміналів. Зараз до послідовного порту приєднують модеми, віддалені принтери, плотери, мишку та інше обладнання.

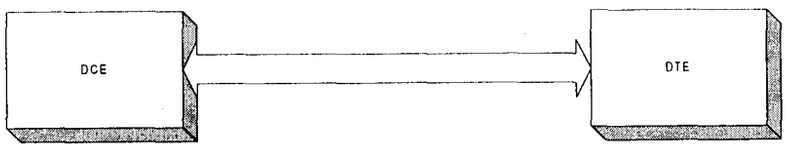


Рис. 4.1. Учасники обміну інформацією через послідовний інтерфейс RS-232C.

У ПК реалізовано до чотирьох послідовних портів (COM1–COM4). Роз'єднувач послідовного порту на панелі ПК має 25 або 9 контактів (найчастіше використовують тільки дев'ять з них). 'Серцем' послідовного порту є мікросхема **UART** (Universal Asynchronous Re-

ceiver/Transmitter). Вона перетворює паралельний код у послідовний та передає його побітно у лінію, додаючи біти старту, зупинки та контролю. Таким чином відбувається асинхронне передавання (див. розділ 3). Через послідовний порт дані можна передавати на відстань до 30 м. Під час передавання даних один з комп'ютерів є *головним* (Data Communication Equipment (**DCE**)), інший – *підлеглим* (Data Terminal Equipment (**DTE**)) (рис. 4.1). Головні сигнали інтерфейсу RS-232C наведені в табл. 4.1.

Таблиця 4.1. Головні сигнали інтерфейсу RS-232C

Сигнал	Контакт DB9	Контакт DB25	Примітка
DCD data carrier set	1	8	Виявлений сигнал-носій. Модем готовий приймати дані
RxD receive data	2	2	Дані на приймання
TxD transmit data	3	3	Дані на передавання
DTR data term ready	4	20	Сигнал готовності
GND ground	5	7	Земля
DSR data set ready	6	6	Модем увімкнено та приєднано до лінії
RTS сигнали	7	4	Готовий до передавання
CTS квитування	8	5	Запит на передавання
RI ring indicator	9	22	Дзвінок

Для передавання даних у найпростішому випадку потрібно тільки три сигнали:

TxD – передати дані; RxD – прийняти дані; GND – "земля".

Решта шість сигналів – допоміжні. Серед них можна виділити сигнали підтвердження RTS, CTS. Використовуючи повний набір сигналів та програмне керування передаванням через переривання BIOS14h, можна будувати різні варіанти протоколів. Швидкості передавання звичайно вибирають з дискретного ряду

50, 75, 110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200 бод.

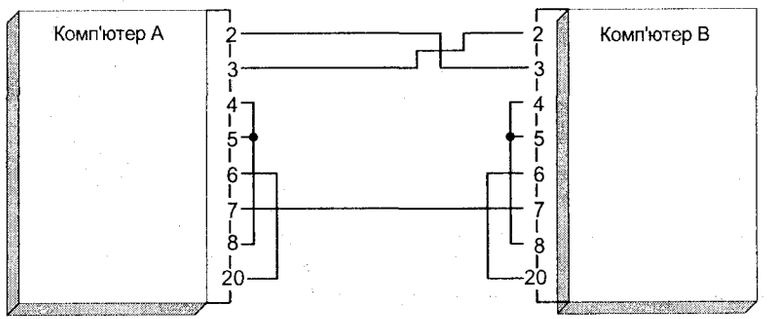


Рис. 4.2. Схема з'єднання контактів нуль-модемного сполучення.

Вони залежать від якості каналу зв'язку. Для ПК IBM PC AT максимальна швидкість становить 9600 бод, для PS/2 – 19200 бод. Мікросхеми UART апаратно розраховані на більші швидкості передавання (UART 8250 (PC, XT, код – 0) – 38400 бод, UART 16550, 16550A (PC AT, коди 1,2) – 115200 бод), однак програмні засоби BIOS значно їх обмежують. Деякі спеціальні програми (Laplink та ін.), які прямо програмують UART, мають максимальну швидкість.

Наприклад, розглянемо передавання даних між двома комп'ютерами через послідовні порти засобами операційної системи MS DOS з використанням нуль-модема. Нуль-модем – це з'єднання двох комп'ютерів через послідовні порти, яке імітує модемне з'єднання. Схема такого з'єднання показана на рис. 4.2.

Для передавання треба ввести на обох комп'ютерах такі режими обміну даними (рис. 4.3).

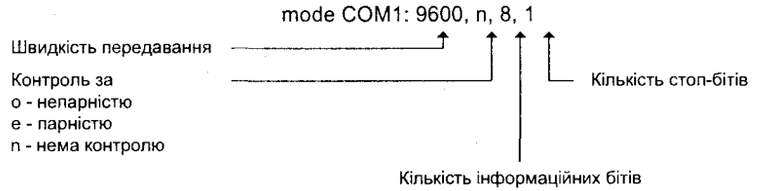


Рис. 4.3. Командний рядок налаштування режиму передавання.

На приймальному комп'ютері треба ввести

COPY COM1: <ім'я файлу>

Приймальний комп'ютер очікує введення. На передавальному комп'ютері треба ввести

COPY <ім'я файлу> COM1:

Після цього відбувається передавання.

Аналогічно з використанням нуль-модема можна передавати дані за допомогою програм Commander Link (NC), Laplink, Brooklyn Bridge.

4.4. Модеми, їхня класифікація

Як відомо, **модем** – це пристрій для передавання та приймання даних з телефонного каналу зв'язку. Є велика кількість різноманітних модемів. Як зорієнтуватися та вибрати потрібний? Для цього треба їх класифікувати. Модеми розрізняють за розміщенням, різновидами каналів, сервісними можливостями, типом передавання, ступенем спеціалізації, набором протоколів.

Розміщення

Модеми бувають внутрішні (які приєднують до роз'єднувача розширення) та зовнішні (які приєднують до послідовного порту). Внутрішні модеми оформлені у вигляді окремої плати,

зовнішні мають свій корпус та розміщені ззовні комп'ютера. Внутрішні модеми займають роз'єднувач розширення комп'ютера, а зовнішні – COM-роз'єднувач. Користувачу ліпше працювати з зовнішнім модемом, оскільки він має додаткові панелі індикації стану передавання інформації, простіший у конфігуруванні та експлуатації. Зовнішні модеми бувають:

- *настільні* – мають автономне живлення;
- *портативні* – менші від настільних;
- у вигляді *карти* інтерфейсу PC Card;
- виконані для *роботи в модемному стояку*.

Різновиди каналів, з якими модеми працюють

Звичайні 'телефонні' модеми передають інформацію комутованими з'єднаннями по телефонному каналу.

Чотирипроводові модеми передають інформацію по чотирьох лініях. Дві лінії використовують для передавання, а дві – для приймання даних. Це дає змогу значно зменшити вплив завад та підвищити швидкість передавання.

Мережеві модеми мають вбудований адаптер локальної мережі, працюють безпосередньо, як вузол локальної мережі (модеми фірми Shiva).

Модеми для швидкісного передавання прямим кабелем (Limited Distance Modem або Short Range Modem (LDM)) використовують не телефонний канал, а пряме проводове сполучення. Тому швидкість передавання в них значно більша. Наприклад, модеми серії 217x Motorola забезпечують на відстані до 15 км швидкість 80 Кбіт/с (для якісних ліній – до 2 Мбіт/с) (див. Д.4.5).

Якщо модем для прямого передавання працює через UART, то швидкість передавання не перевищує швидкості роботи UART.

Радіомодеми передають пакети інформації в діапазоні частот радіотелефону, мають вбудований радіопередавач.

Стільникові модеми призначені для передавання інформації в стільниковій телефонній мережі. Працюють у винятково несприятливих умовах (трясіння, зміна амплітуди сигналу, завади, тимчасове щезання сигналу, його відбивання). Використовують спеціальні протоколи.

На базі радіо- та стільникових модемів будують безпроводові мережі.

Сервісні можливості

Факс-модеми (з інтегрованою можливістю приймати та передавати факс-повідомлення).

Звукові модеми (дають змогу записувати мовлення з каналу та відтворювати його).

Модеми одночасного передавання мовлення та даних (Simultaneous Voice and Data (SVD)).

Типи передавання

Розрізняють асинхронні та синхронні модеми. Найпоширенішими є асинхронні модеми для передавання даних комутованими телефонними лініями. Синхронні модеми передають дані між мейнфреймами, а також у мережах X.25. Як звичайно, усі професійні модеми синхронні.

Ступінь спеціалізації

Модеми бувають дешеві широкого використання та дорогі мережеві. Мережеві модеми, як звичайно, виготовляють комплектами. Вони забезпечують як доступ абонентів до мережі, так і міжвузлові та міжмережеві зв'язки. Мережеві модеми передають інформацію пакетами і надають користувачу значно більший обсяг послуг, ніж модеми широкого використання. Мережеві модеми можуть також реалізовувати дво- та чотирипроводове передавання, виконувати мультиплексування даних.

Набір протоколів

Набір протоколів визначає швидкість передавання даних модема, алгоритми виправляння помилок, сумісність та можливість роботи з модемами інших виробників. Це головний параметр вибору модема.

Частота-носій телефонного кабелю становить 3000 Гц, максимальна швидкість передавання – 2400 бод. Це обмежує подальший розвиток модемних технологій. З широким розповсюдженням мереж ISDN (швидкість передавання – 2·64 Кбіт/с), а в перспективі і мереж ATM (швидкість передавання необмежена, сьогодні – 150–600 Мбіт/с), модем, як засіб передавання відійде у минуле.

4.5. Керування модемом

Сучасний модем – це складний технічний пристрій, яким можна керувати з ПК, якщо посилати на нього коди керування. Як звичайно, модем має два режими роботи:

- командний;
- передавання даних.

Керувати модемом можна у командному режимі. Коди керування модемів різні, однак є один загальноприйнятий стандарт, розроблений фірмою Hayes на початку 80-х років. Його підтримують більшість модемів, їх ще називають *Hayes-сумісними*. Майже всі команди модема починаються з комбінації AT (Attention – Увага!). Наведемо приклади деяких команд:

ATZ	Налаштування початкових значень
ATDT#	Тональне набирання телефонного номера

ATDP#	Імпульсне набирання телефонного номера
AT&F	Завантаження 'фабричних' параметрів модема
AT&W	Записування поточних значень параметрів у пам'ять модема. Ці значення діють у випадку поновного ввімкнення модема або виконання команди ATZ.

Увімкнувши модем, його треба спочатку налаштувати. Для цього використовують послідовність команд, записану в рядку ініціалізації. Для кожного типу модема може бути свій рядок ініціалізації. У командах ініціалізації треба також враховувати тип телефонної станції, тип модема, з яким налаштовують зв'язок. Більшість виробників постачають апаратно зашиту в модем 'фабричну' послідовність ініціалізації, яку викликають командою AT&F.

4.6. Передавання даних у двопроводовій лінії з використанням модема

Розглянемо приклад організації передавання даних між двома ПК через модеми по призначених лініях (рис. 4.4).

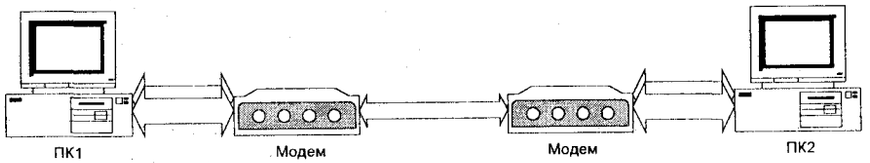


Рис. 4.4. Схема сполучення.

У цьому випадку відбуваються такі дії (рис. 4.5):

- на першому ПК користувач уводить інформацію для передавання та натискає на клавішу Enter;
- ПК користувача надсилає на модем сигнал *Запит на передавання*;
- перший модем сприймає цей сигнал та надсилає телефонною лінією сигнал-носій (carrier). Його генерує модем, а не телефонна служба;
- другий модем приймає цей сигнал, синхронізує свій приймач і повідомляє другий ПК про його виявлення;
- перший модем очікує деякий час, щоб дати змогу другому модему виявити сигнал-носій, і надає першому ПК сигнал *Готовий до передавання*;
- ПК передає на модем блок даних, який модулює сигнал-носій та передає його лінією другому модему;
- другий модем демодулює сигнал, одержує дані та передає їх своєму ПК;
- другий ПК приймає дані від модема;
- коли перший ПК закінчив передавання, він знімає сигнал *Запит на передавання*;

- перший модем виявляє зникнення сигналу *Запит передавання* та перестає передавати в канал сигнал-носій;
- другий модем виявляє його зникнення і через деякий час знімає сигнал *Виявлення сигналу-носія*, який передавав другому ПК.

Отже, передавання закінчилося.

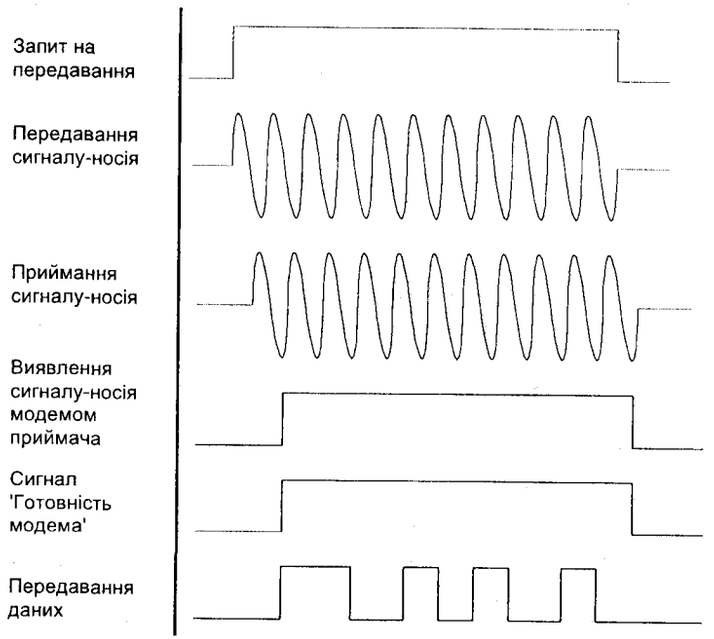


Рис. 4.5. Набір сигналів.

Якщо зв'язок іде комутованими лініями, то передавання відбувається аналогічно, але перед його початком налагоджують сполучення за таким порядком:

- ініціалізують послідовний порт;
- попередньо налагоджують модем;
- коли модем перебуває в командному режимі, програма надсилає сигнал DTR про готовність до передавання даних;
- оператор задає в командному рядку команду налагодження сполучення з певним телефонним номером;
- модем виконує команду, налагоджує сполучення з віддаленим модемом, переходить у режим передавання даних та подає сигнал DSR; видається сигнал DCD;
- програма надсилає сигнал RTS про готовність до передавання, модем – сигнал CTS про готовність до приймання. Відбувається передавання.

Отже, під час налаштування сполучення та передавання даних використовують спеціальні сигнали та команди підтвердження готовності до приймання або передавання. Ці сигнали можуть бути апаратними або програмними. В інтерфейсі модем – локальний комп'ютер застосовують апаратні сигнали DTR/DSR під час налаштування сеансу зв'язку та апаратні RTS/CTS під час передавання кожного інформаційного кадру. У ланці модем–модем неможливість використання більш швидкодійних апаратних сигналів зумовлює потребу обмінюватися спеціальними байтами підтвердження (XON/XOFF).

Звичайні модеми застосовують з такою метою: додзвонювання (автоматичне набирання номера), обмін файлами, обмін текстом у реальному масштабі часу, керування віддаленим комп'ютером, емуляція термінала, доступ до електронних дощок оголошень (BBS), доступ до глобальних мереж, віддалене використання локальної мережі.

4.7. Стандарти модемів

Усі модемні стандарти можна розділити на три групи: протоколів передавання даних, корекції помилок, стиснення. За рівнем розповсюдження та сумісності з іншими стандартами розрізняють міжнародні стандарти, фірмові протоколи, що стали стандартом де-факто, а також малопоширені фірмові розробки.

Стандарти передавання даних

Таблиця 4.2. Стандарти передавання даних модемом

Тип	Протокол	Швидкість, Кбіт/с	Дуплекс	Лінія	Метод модуляції	Примітка
Низькошвидкісні < 2.4 Кбіт/с	V.21 V.22	0.3 1.2	СЧ СЧ	К К,2	FSK DPSK	Висока завадостійкість
Середньошвидкісні 2.4-9.6 Кбіт/с	V.22bis V.32	2.4 9.6	СЧ СЕ	К К,2	QAM QAM, TCM	Уперше реалізовано пригнічення луни-сигналу
Швидкісні > 9.6 Кбіт/с	V.32bis	14.4	СЕ	К,2	TCM	Можна динамічно перемикати швидкість залежно від якості лінії. Якість лінії визначають за співвідношенням сигнал/шум, або за відсотком помилкових блоків
	V.33 V.34 V.90	14.4 28.8 56	С СЕ С	4 К,2 К,2	TCM	

Примітки. Режими: С – симетричний; А – асиметричний; Ч – з розподілом частоти; Е – з пригніченням луни-сигналу; лінії: К – комутовані; 2 – двопроводові з призначеним каналом; 4 – чотирипроводові з призначеним каналом. Методи модуляції: **FSK** (Frequency Shift Keying) – частотна модуляція, найнадійніша; **DPSK** (Different Phase Shift Keying) – фазова модуляція. Використовують, якщо бод (див. Д.4.4) кодує до 3 бітів. Після цього розпізнавання погіршується; **QAM** (Quadrature Amplitude Modulation) – квадратурна амплітудна модуляція (амплітудно-фазова). Кодують до 8 бітів на бод; **TCM** (Trellis Coded Modulation) – модуляція з ґратковим кодуванням та уведенням надлишковості. Кожний бод несе додатковий біт, що допомагає поновити інформаційні біти. Для кодування використовують QAM.

Додаткова інформація про стандарти.

Низькошвидкісні стандарти

Bell 103j – 300 біт/с
Bell 212a – 1200 біт/с
V.22 – 1200 біт/с
V.22 bis – 2400 біт/с

Стандарти Bell прийняті в США, стандарти V.22, V22bis – ITU. Передавання даних дуплексне для двопроводових ліній зв'язку. У стандарті V22bis дані групуються по 4 біти і передаються зі швидкістю 600 бод.

Середньошвидкісні стандарти

Bell 208 – 4800 біт/с
V.29 – 9600 біт/с
V.33 – 14400 біт/с

Ці стандарти специфікують передавання даних призначеними чотирипроводовими лініями, їх використовують зрідка.

V.32 – 9600 біт/с

Стандарт V.32 діє з 1984 р. для звичайних двопроводових комутованих ліній. Дані в ньому групуються по 4 біти і передаються зі швидкістю 2400 бод. Цей стандарт дає змогу обом модемам передавати дані одночасно. Для його реалізації розроблено спеціальний сигнальний процесор, який компенсує луна-сигнали (див. Д.4.3), та поліпшено техніку фазового матричного кодування, яка значно зменшує рівень помилок.

У 1989 р. прийнято стандарт

V.32bis – 14400 біт/с,

який є розширенням до V.32 з сильнішою компенсацією луна-сигналу. Висока швидкість передавання досягається, якщо висока якість ліній зв'язку. Дані групуються по 6 біт і передаються зі швидкістю 2400 бод (про групування даних див. Д.4.4).

З 1994 р. діє стандарт

V.34 – 28800 біт/с.

Порівняно з V.32bis у ньому введено низку нових вирішень.

• *Попереднє кодування (precoding)*. У швидкісних модемах широко використовують метод адаптивної корекції, який компенсує тремтіння фази та коливання рівня сигналу. Однак адаптивна корекція інколи призводить до посилення шуму в каналі. Процедура попереднього кодування дає змогу змінити сигнал таким чином, щоб запобігти цьому.

• *Багатовимірне кодування (multidimensional coding)*. Кожен символ, що його передає модем, складається з певної кількості бітів. Чим більше обчислювальних ресурсів має модем, тим більше бітів на один символ він зможе передати. Наприклад, модем стандарту V.32bis передає 6 бітів на символ зі швидкістю 2400 симв/с. Модеми стандарту V.34 передають 9 бітів на символ зі швидкістю 3200 симв/с.

• *Нелінійне кодування (nonlinear coding)* використовують для збільшення відстані між піками сигналів, що робить їх стійкішими до спотворення (пор. з поняттям кодова відстань).

• *Тестування лінії (line probing)*. Перед та під час роботи перевіряється якість лінії та адаптивно вибирається швидкість передавання.

• *Ліпші апаратні вирішення*. Модем має ліпші аналого-цифровий та цифро-аналоговий перетворювачі (АЦП/ЦАП) з підвищеною роздільною здатністю (сигма-дельта перетворення), більшу ємність пам'яті, використано нове покоління сигнальних процесорів, які виконують до 1000–2000 обчислень на один біт, тоді як у модемі V.32 виконувалося 200–300 обчислень.

З 1998 р. діє стандарт

V.90 – 56000 біт/с

Швидкість передавання у модемах стандарту V.90 збільшується тільки у випадку низхідного передавання (сервер → клієнт) унаслідок вилучення етапу аналого-цифрового перетворення сигналу на шляху від сервера до клієнта. У цьому випадку АТС на зворотному шляху сигналу повинні бути цифровими. Підвищення швидкості досягається завдяки зменшенню шуму, який створював АЦП. У прямому каналі (між клієнтом та сервером) швидкість відповідає стандарту V.34.

Стандарти виправлення помилок

MNP 2–4
V.42

Стандарти MNP 2–4 розроблені фірмою Microcom і призначені для виправлення помилок. MNP 2 – байтова процедура (для обчислення контрольної суми (Cyclic Redundancy Check (CRC)) послідовно беруться байти даних). MNP 3 – бітова процедура, послідовність бітів не ділиться на байти. MNP 4 – це надбудова над MNP 2, 3, яка їх використовує.

Стандарт V.42 (1988) регламентує виправлення помилок за методом повторення запитів. Дані групуються в блоки. Правильність передавання перевіряється підрахунком контрольної суми. В основі стандарту V.42 є протокол **LAPM** (Link Access Procedure for Modem). Це бітовий протокол, що використовує підмножину протоколу канального рівня HDLC (див. розділ 8). Під час налагодження сполучення модем пробує працювати на LAPM. Якщо ж це не вдається, то переходить на MNP.

Стандарти ущільнення інформації

MNP 5
V.42bis

Протоколи динамічного пакування/розпакування даних обов'язково працюють разом з відповідними протоколами виправлення помилок. Вони використовують різні модифікації алгоритмів Лемпеля-Зіва.

Протокол MNP 5 працює з протоколами MNP 2–4. Однак сучаснішим є протокол стандарту V.42bis, який можна реалізувати тільки зі стандартом V.42. Середній коефіцієнт ущільнення у ньому становить 4. Автоматично простежується ступінь ущільнення даних, якщо дані вже ущільнені, то вдруге їх ущільнити не можна.

Асинхронний повнодуплексний зв'язок

Інколи виникає потреба налаштувати один швидкісний (9600 біт/с) прямий інформаційний канал та повільний зворотний (300 біт/с). У цьому випадку не виходять за межі перепускної здатності телефонного каналу, а також не треба дорогих схем корекції луна-сигналів. Така технологія одержала назву **HST** (High Speed Technology) фірми US Robotics. У 1989 р. US Robotics удосконалила HST технологію: прямий канал має швидкість 14400 біт/с, зворотний – 450 біт/с. HST стала стандартом для електронних дощок оголошень BBS.

Стандарти протоколів для стільникових модемів

Усі відомі протоколи для стільникових модемів суміщують функції протоколів передавання даних та виправлення помилок. Працюють вони у винятково несприятливих умовах, з постійними змінами швидкості передавання та розміру блоку (V-протоколи не забезпечують динамічної зміни розміру блоку).

Прикладами таких протоколів є MNP 10 (перший стільниковий протокол, що давав змогу динамічно змінювати швидкість та розмір блоків) та сучасніша розробка **ETC** (Enhanced Throughput Cellular) компанії AT&T Paradyne. Він є розширенням протоколів V32bis та V42bis.

Стільникові модеми та протоколи можна використовувати і в звичайних лініях, особливо якщо є значні завади.

Бібліографія та джерела

1. *Бараш Л.* Быстрые байты в телефонной сети // Комп'ютерное обозрение. 1998. № 5 (124).
2. *Вильховченко С.* Модем-96. М.: ABF, 1995.
3. *Минкин Э.Б.* Анатомия модемных 56-К технологий // Сети и системы связи. 1997. № 8, 9.
4. *Форсюк В.* Modem Guide. Модемы. Справочное руководство. К.: Евроиндекс Л.т.д., 1994.
5. *Хаусли Т.* Системы передачи и телеобработки данных. М.: Радио и связь, 1994.

ДОДАТКИ ДО РОЗДІЛУ 4

Д.4.1. Інтерфейси RS-422/423/449

Інтерфейс RS-232C має суттєві обмеження щодо швидкості та відстані передавання. З метою його удосконалити EIA розробила нові інтерфейси RS-423 та RS-422; ITU – V.10, X.26 (RS-423) та V.11, X.27 (RS-422). Порівняльна характеристика цих стандартів наведена в табл. Д.4.1.

Таблиця Д.4.1. Порівняльна характеристика інтерфейсів

Швидкість передавання, Кбіт/с		Довжина кабелю, м
RS-423, V.10, X.26	RS-422, V.11, X.27	
1	100	1000
10	1000	100
100	10000	10

EIA RS-423, як і RS-232C, визначає характеристики *несиметричного* цифрового інтерфейсу.

EIA RS-422 визначає *симетричний* цифровий інтерфейс і забезпечує більші швидкості передавання даних та ліпший захист від завад. (Пояснення різниці між несиметричним та симетричним інтерфейсом див. Д.4.2)

EIA RS-449 доповнює RS-423/422 описом сигналів, роз'єднувачів тощо (аналогічно до того, як V.28 доповнює V.24).

Д.4.2. Симетричні та несиметричні цифрові інтерфейси

У *несиметричних* цифрових інтерфейсах усі 'прямі' сигнальні проводи мають один зворотний провід ('землю') (рис. Д.4.2.1). У випадку спотворення сигналу завадою рівень сигналу-'землі' є незмінним. Значення читається як різниця між сигналом на прямому проводі та 'землі'. Отже, вплив завад під час передавання несиметричним інтерфейсом значний.

У *симетричному* цифровому інтерфейсі (рис. Д.4.2.2) для передавання кожного сигналу є два проводи – 'прямий' та 'зворотний'. Передавання та читання інформації відбувається в *диференційному режимі*, тобто корисний сигнал читається як різниця сигналів у двох проводах. Пара проводів скручена разом, так що завади впливають на них однаково.

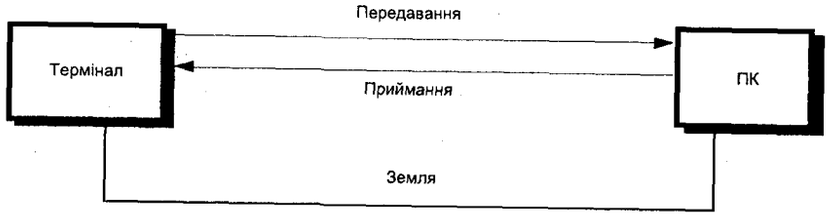


Рис. Д.4.2.1.Несиметричний інтерфейс.

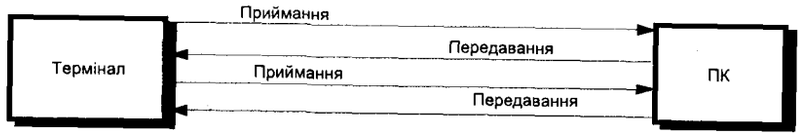


Рис. Д.4.2.2. Симетричний інтерфейс.

Симетричні та несиметричні ланки розміщують в одному кабелі. У цьому випадку сигнали, які часто змінюються, такі як *Дані, що передаються*, *Дані, що приймаються*, дані синхронізації, доцільно передавати симетричними ланками, а сигнали, що змінюються зрідка (*Запит передавання*, *Готовність до передавання*), – несиметричними.

Д.4.3. Компенсація луни

Під час передавання сигналу телефонною мережею стикаються з явищем **луни** (рис. Д.4.3.1).

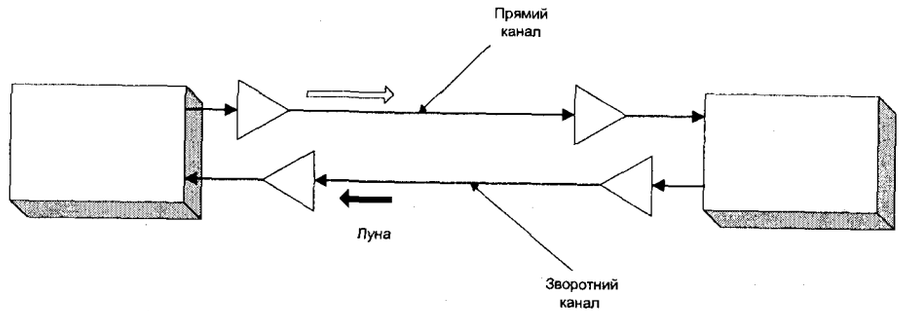


Рис. Д.4.3.1. Виникнення луни.

У цьому випадку прямий сигнал проходить лінією до місця призначення, відбивається і йде в зворотному напрямі. Під час 'прямого' та 'зворотного' проходження він посилюється і потрапляє назад, накладаючись на первинний сигнал. Якщо загальна відстань передавання невелика, то луну не розрізняють. Однак якщо проміжними є супутникові канали з великою затримкою, то вплив луни стає значним. Крім того, луна, що передається каналом зв'язку, використовує деяку частину його перепускної здатності.

Особливо важливо зменшити вплив луни під час передавання даних. З цією метою можна використовувати спеціальні прилади, які по черзі блокують передавання в прямому та зворотному напрямах. У сучасних системах для компенсації луни застосовують електронні засоби, які очищають корисний сигнал від луна-сигналу.

Д.4.4. Групування даних

Телефонні канали, якими передають дані за допомогою модема, були первинно спроектовані для передавання аналогового сигналу мовлення. Відомо, що діапазон сигналу мовлення становить 30–15000 Гц. Проте головна частина сигналу припадає на діапазон 300–3400 Гц. Смуга перепускання телефонного каналу – 3100 Гц. Для передавання даних зі швидкостями понад 3000 біт/с потрібно за один період модуляції передавати кілька бітів.

Швидкість, виміряна за частотою зміни сигналу-носія, дає ***швидкість передавання в бодах****. Якщо за один період модуляції передається 1 біт, то швидкості передавання, виміряні в бодах і в бітах на секунду, збігаються. Однак це справджується тільки для низькошвидкісних модемів (до 1200 біт/с).*

Відомо, що модеми, у яких швидкість становить 4800 біт/с, передають 3 біти за період з частотою 1600 Гц, модеми, у яких швидкість 9600 біт/с, передають 4 біти за період з частотою 2400 Гц. Як же відбувається подібне групування даних?

Наприклад, модем, у якому швидкість 2400 біт/с, за період передає 2 біти. Для кожної з чотирьох можливих комбінацій значень цих бітів відповідає зсув фази у випадку фазової модуляції сигналу-носія (відповідно на 0°, 90°, 180°, 270°). У модемах, де швидкість становить 4800 біт/с, кількість зсувів фази досягає вже восьми. У модемах з більшими швидкостями, унаслідок технічних труднощів детектування невеликих зсувів фаз, використовують **квадратурну амплітудну модуляцію** – комбінацію восьми фаз та чотирьох значень амплітуд (у модемах на 9600 біт/с).

Д.4.5. Модеми для фізичних ліній

Модеми для фізичних ліній (МФЛ) – це апаратура передавання даних по призначеній ненавантаженій мідній парі на відстань до 40 км. В англійській термінології для позначення цих модемів є терміни *baseband modem, short-range modem, limited distance modem, line driver, short-haul modem.*

Якщо мідними проводами з'єднати персональні комп'ютери напряму (без телефонних комутаторів та фільтрів), то дані можна передавати зі швидкістю до 50 Мбіт/с. За даними консорціуму ADSL Forum максимальна дальність передавання цифрового сигналу по одній парі мідного дроту діаметром 0.5 мм на швидкості 1.544 Мбіт/с становить 6 км, а на швидкості 2 Мбіт/с – 5 км.

Отже, МФЛ забезпечують невелику дальність зв'язку, гальванічну розв'язку щодо заземлення між пунктами, досить високу швидкість передавання.

МФЛ не виконують функцію модуляції/демодуляції, а тільки кодують сигнали. Вони потребують широкої смуги перепускання (не менше 80 МГц) та використовують усю смугу допустимого спектра частот, не дають змоги частотно розподіляти канали.

Одне з обмежень за швидкістю – телефонні комутатори АТС та встановлені там фільтри (4 кГц).

Класифікація МФЛ:

- дешеві модеми зі швидкістю передавання до 160 Кбіт/с та недостатньо новими алгоритмами кодування;
- дорогі модеми зі швидкостями близько 2 Мбіт/с. У них часто використані досить дорогі технології xDSL (див. розділ 28).

МФЛ застосовують для налагодження зв'язку на 'останній милі'.

ПЕРЕДАВАННЯ ДАНИХ З ВИКОРИСТАННЯМ АДАПТЕРА

Загальна характеристика та класифікація адаптерів. Будова та складові частини адаптера. Робота адаптера під час приймання та передавання даних. Конфігурування та налагоджування. Тенденції розвитку адаптерів. Передавання даних через паралельний порт. Джерела безперебійного живлення.

5.1. Загальна характеристика і класифікація адаптерів

Адаптери станцій локальних мереж безпосередньо приєднують до внутрішньої шини введення-виведення ПК. Вони дають змогу досягти значно більших швидкостей передавання, ніж через послідовний чи паралельний порти. (Фактично швидкість передавання обмежена швидкістю внутрішньої шини процесора). В адаптерах, як звичайно, апаратно реалізовані протоколи фізичного та канального рівнів еталонної моделі взаємодії відкритих систем.

Адаптери різних мереж виробляють багато фірм. Вибираючи адаптер будь-якої фірми, треба звернути увагу на такі його характеристики:

- до якої мережі він належить (Ethernet, Arcnet, Token Ring, FDDI та ін);
- яку розрядність (8, 16, 32) має та до якої шини (ISA, EISA, PCI, MCA) приєднується;
- яку має потужність та які алгоритми використовує (розрізняють адаптери для робочих станцій, серверів);
- які він має роз'єднувачі та до якого кабельного середовища ЛМ приєднується.

Роз'єднувачі бувають такі:

BNC – для приєднання тонкого коаксіального кабелю;
AUI – для приєднання товстого коаксіального кабелю;
RJ45 – для приєднання скрученої пари;
MIC, ST, SC – для приєднання волоконно-оптичного кабелю.

5.2. Будова та складові частини адаптера

Розглянемо головні складові частини та особливості роботи адаптера ЛМ на прикладі адаптера NI 5210 для мережі Ethernet фірми Interlan Inc (рис. 5.1).

Центральною частиною адаптера є **співпроцесор INTEL 82586** який виконує деякі функції опрацювання інформаційних кадрів протоколу канального рівня. Співпроцесор кодує інформацію перед передаванням у мережу, декодує її після приймання, виявляє та виправляє помилки, повідомляє центральний процесор про надходження інформації, виконує головні функції з реалізації MAC підрівня протоколу канального рівня. Використання спеціалізованого процесора дає змогу розвантажити ЦП та підвищити загальну швидкодію системи.

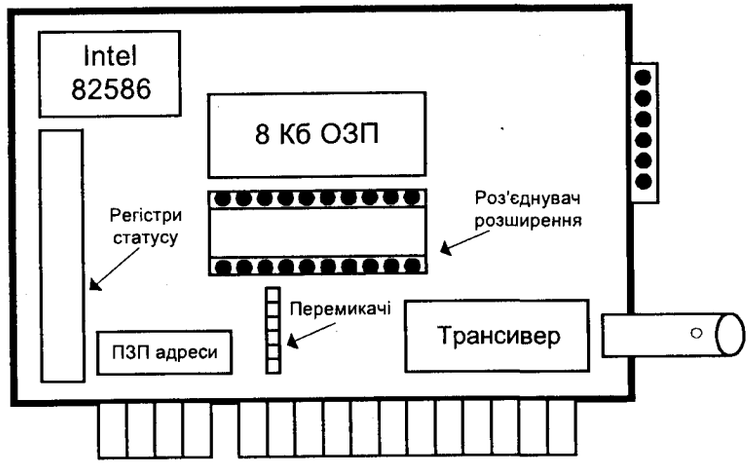


Рис. 5.1. Головні частини адаптера.

Важливою частиною адаптера є **оперативна пам'ять** (8 Кбайт). У цю пам'ять записують інформацію перед передаванням і після приймання. Пам'ять відображається на адресний простір комп'ютера (параметр Base Memory Address). Її може одночасно читати і записувати як ЦП, так і мережевий співпроцесор.

У **роз'єднувач розширення** можна приєднати додаткову мікросхему пам'яті або мікросхему постійної пам'яті (ПЗП) для автоматичного завантаження комп'ютера через мережу.

Вісім регістрів стану та керування дають змогу ЦП та співпроцесору обмінюватися командами. Регістри перенумеровані за їхнім зміщенням від базового значення (параметр I/O Base Adress) – від 00h до 07h.

ПЗП адреси для адаптерів мережі Ethernet містить унікальну мережеву адресу комп'ютера, встановлену фірмою-виробником адаптера. Жодна з цих адрес не може повторитися. Кожна фірма-виробник має адреси з певного діапазону. Довжина фізичної адреси для мережі Ethernet – 48 біт.

Перемикачі дають змогу конфігурувати параметри адаптера (див. 5.4).

Кабельні роз'єднувачі призначені для приєднання адаптера до мережі. В адаптері, який розглядаємо, є два роз'єднувачі для приєднання адаптера до тонкого (BNC-роз'єднувач) або до товстого (AUI-роз'єднувач) Ethernet.

Крім того, на платі адаптера також розміщено **трансивер** (приймач-передавач) для роботи з тонким Ethernet. Товстий Ethernet використовує зовнішній трансивер.

Роз'єднувач приєднання до системної шини ПК. Роглянувши форму роз'єднувача, кількість та конфігурацію контактів, можна визначити розрядність адаптера та тип шини, для якої він спроектований.

5.3. Робота адаптера під час приймання та передавання даних

Передавання даних. Комунікаційне програмне забезпечення будує кадри Ethernet та записує їх у пам'ять адаптера. У регістри керування та стану записується команда передати кадр, адреса та кількість інформації для передавання. Мережевий співпроцесор аналізує значення регістрів, бере кожен кадр, опрацьовує його згідно з вимогами протоколу і передає у мережу.

Приймання даних. Мережевий співпроцесор постійно стежить через трансивер за кадрами в мережі та виділяє ті, які призначені для конкретного адаптера. У випадку надходження такого кадру співпроцесор перевіряє правильність даних, розміщує їх у пам'яті, записує в регістри керування команду приймання даних, адресу їх розміщення у пам'яті і видає для центрального процесора переривання з визначеним номером. ЦП та комунікаційне ПЗ відкидає службові дані, аналізує прийняті дані та переміщує їх в головну пам'ять.

5.4. Конфігурування адаптера

Конфігуруванням адаптера задають такі параметри:

- **I/O Base Address** – адреса пам'яті, куди відображаються регістри стану та керування;
- **Base Memory Address** – адреса пам'яті, куди відображається внутрішня пам'ять адаптера;
- **IRQ** – номер переривання, за яким ЦП повідомляють про прийняті дані.

Конфігурування адаптера відбувається шляхом задання значень параметрів з використанням перемикачів. Сучасні адаптери, як звичайно, не мають перемикачів, їх конфігурують спеціальними програмами, доданими до адаптера. Адаптери, що відповідають вимогам стандартів Plug and Play, можна конфігурувати автоматично засобами операційної системи. Для збільшення швидкості пересилання інформації часто використовують механізми *прямого доступу до пам'яті (Direct Memory Access (DMA))*. Номер каналу DMA у цьому випадку – це ще один параметр конфігурування адаптера.

5.5. Тенденції розвитку адаптерів

Визначальним для сучасної епохи є перехід від класичних мереж зі швидкістю близько 10 Мбіт/с до швидкісних, що передають дані зі швидкістю 100 та 1000 Мбіт/с. Використання в одній мережі різношвидкісних технологій передбачає, щоб адаптери підтримували функцію *автоузгодження*, тобто автоматично узгоджували швидкість передавання зі своїм партнером (див. Д.6.1). Високі вимоги щодо швидкості зумовлюють і зміни в структурі адаптерів. Розглянемо, наприклад, мережу Gigabit Ethernet. ПК з 32-розрядною PCI шиною здатні передавати трафік 1 Гбіт/с, а адаптери з 64-розрядною шиною – 2 Гбіт/с. Водночас з такою швидкістю можна завантажити практично 100% ресурсів ЦП. На виконання інших завдань не залишиться ресурсів. Тому адаптери Gigabit Ethernet мають вбудований RISC процесор, що виконує інтелектуальні функції вивантаження, які налагоджені на параметри конкретного комп'ютера. Дані з мережі відразу надходять у пам'ять і відразу ж стають доступними для застосувань. Щоб зменшити завантаженість ЦП, регулюють співвідношення кількості переривань до обсягу отриманої інформації. За одне переривання приймається велика кількість кадрів. Співвідношення кількості кадрів на одне переривання можна задати вручну або автоматично. Це дає змогу створити 'адаптивні' переривання, частота яких залежить від завантаження.

5.6. Передавання даних через паралельний порт

Розглянемо паралельний порт стандарту *Centronics*, який звичайно використовують для приєднання принтера, стримера та інших периферійних пристроїв. Теоретична максимальна швидкість передавання даних через цей порт – 500 Кбіт/с, реально – не більше 200 Кбіт/с. Довжина кабелю – до 3 м. Буфер має ємність 64 байти. Отже, передавання через паралельний порт, незважаючи на обмеження, удвічі швидше, ніж через послідовний.

У 1992 р. IEEE затверджено швидкісний стандарт передавання даних через паралельний порт (стандарт *EPP*). Він дає змогу передавати дані через двонапрямлений порт *Fast Centronics* зі швидкістю 2 Мбіт/с. У цьому випадку використовують DMA – прямий доступ до пам'яті. Пізніше з'явився стандарт *ECP (Zippy)*, який також використовує порт *Fast Centronics*, однак має інший алгоритм ущільнення.

На практиці використання паралельних портів для передавання даних в комп'ютерних мережах непоширене (головним чином, їх застосовують для прямого сполучення комп'ютерів).

5.7. Засоби приєднання до мережі

На кінці коаксіального кабелю мережі Ethernet кріплять спеціальний пристрій – *термінатор*, який узгоджує хвильовий опір до 75 або 50 Ом. Аналогічні заходи щодо узгодження застосовують і в інших мережах.

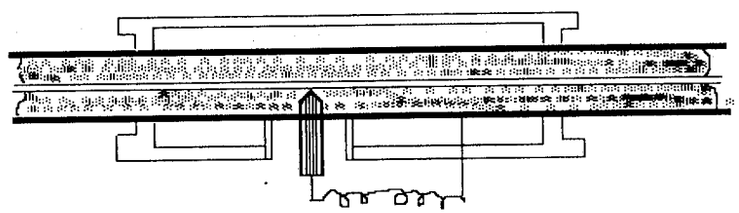


Рис. 5.2. Контакт з проколюванням ізоляції.

Приєднання розгалужувача до кабелю залежить від типу кабелю і може бути розривним або нерозривним. Зокрема, у мережі Ethernet, що має 'товстий' коаксіальний кабель, для при-

єднання до кабелю використовують механічний блок з проколюванням ізоляції (рис. 5.2) (так званий вампірський контакт (vampire tap)).

Оскільки опір у місці контакту голки визначити важко, то доводиться виконувати регулювання з узгодженням загального опору.

Особливе місце посідають волоконно-оптичні кабелі. До них можна приєднатися тільки без розриву. Тому використовують розгалужувачі, які сприймають зміни світла і перетворюють їх у зміни напруги або струму.

5.8. Джерела безперебійного живлення

Джерела безперебійного живлення (Uninterrupted Power Supply – (**UPS**)) застосовують для живлення файл-серверів та інших пристроїв з важливою інформацією. Фірма Novell для своїх систем обумовлює:

"Будь-який файл-сервер та його тверді диски повинні бути приєднаними до апробованого Novellom'ом джерела безперебійного живлення. Ми також рекомендуємо UPS-захист робочих станцій".

Джерела безперебійного живлення виробництва різних фірм мають різну потужність та сервіс. Потужність змінюється від 300–400 до 3000–5000 ВА. Чим більша потужність, тим більшу кількість комп'ютерів можна приєднати, тим триваліша робота після вимкнення живлення. Джерела безперебійного живлення живляться з батарей. Завдяки їм комп'ютер у випадку вимкнення головного живлення працюватиме ще деякий час (від 15 хв до кількох годин). UPS стежать за формою струму живлення, коректують його, дають спеціальні попередження на комп'ютери, ведуть статистику стану живлення тощо. Вартість UPS може коливатися від 200–300$ для дешевих до 1000–3000$ для дорогих UPS. Найвідомішою фірмою, яка виготовляє UPS, є APC (American Power Conversion).

Бібліографія та джерела

1. *Овчинников В.В., Рыбкин И.И.* Техническая база интерфейсов локальных вычислительных сетей. М.: Радио и связь, 1989.
2. *Райс Л.* Эксперименты с локальными сетями микро-ЭВМ. М.: Мир, 1990.

ПРОТОКОЛИ ФІЗИЧНОГО ТА КАНАЛЬНОГО РІВНІВ

Протоколи фізичного рівня. Протокол ECMA-80, ECMA-81. Сервіс протоколів фізичного рівня. Визначення моноканалу та мережі з ретрансляцією. Протоколи канального рівня. Призначення. Підрівні керування доступом до передавального середовища та керування логічним каналом. Стандарти IEEE-802.

6.1. Протоколи фізичного рівня

Протокол фізичного рівня визначає електричні характеристики, які будь-яка система повинна мати у точці приєднання до середовища передавання. Крім того, він описує головні різновиди сервісу фізичного рівня.

Індикація спотворень під час передавання. Спотворення виникають, коли дві або більше станцій передають інформацію одночасно. Тому на фізичному рівні відбувається постійне прослуховування каналу і повідомлення про наявність спотворень.

Контроль часу передавання кадру. Виконується для усунення збоїв, спричинених появою необмеженої послідовності бітів. Для цього фізичний рівень перериває передавання, якщо воно триває понад 150 мс.

Передавання блоків даних.

Автоузгодження швидкості передавання. Сервіс автоузгодження швидкості передавання на фізичному рівні дає змогу партнерам зв'язку обмінятися інформацією про технології, які вони підтримують, та вибрати прийнятний варіант передавання (див. Д.6.1).

Труднощі в стандартизації протоколів фізичного рівня зумовлені великою різноманітністю середовищ передавання, кодів, методів доступу, технічних реалізацій тощо. Тому стандарти фізичного рівня є різні. Наприклад, для великих, багатовузлових, глобальних мереж, а також ЛМ з багатьма вузлами на фізичному рівні використовують протоколи X.21, X.21bis, X.25. Ці протоколи забезпечують реалізацію інтерфейсів кінцевої апаратури передавання даних і апаратури передавання даних телефонними каналами з використанням модемів.

Стандарт ECMA-80 визначає параметри та характеристики фізичного середовища моноканалу.

> ***Моноканал** – це така мережа, в якій фізичне середовище забезпечує одночасне (з точністю до часу поширення сигналу) передавання блоків даних усім приєднаним абонентам.*
>
> *На відміну від моноканалу, у **мережах з ретрансляцією** блоки даних приймаються в проміжних вузлах, а потім знову передаються.*

ECMA-80 ставить вимоги до:

- електричних та фізичних характеристик кабелів і термінаторів;
- правил конфігурування фізичного середовища;
- способів прокладання кабелів.

Згідно з цим стандартом довжина кабелю не може перевищувати 500 м. Загасання в кабелі допускається не більше 8.5 Дб при частоті 10 МГц. Швидкість поширення сигналу не може бути меншою, ніж 0.77 від швидкості світла у вакуумі.

Комплементарним до ECMA-80 є стандарт ECMA-81, який визначає протокол фізичного рівня системи, що взаємодіє з моноканалом.

Стандарт ECMA-90 описує керування доступом до фізичних засобів з'єднання, протокол фізичного рівня та фізичні засоби з'єднання для широкосмугового поліканалу.

6.2. Протоколи канального рівня

Стандарти КМ описують, як звичайно, групу протоколів канального, фізичного рівнів та параметрів передавального середовища.

На сучасному етапі канальний рівень протоколу розділяють на два підрівні (рис.6.1): **керування логічним каналом** (Logical Link Control (LLC)) та **керування доступом до середовища** (Media Access Control (MAC)). Перший забезпечує керування логічним каналом і не залежить від фізичного середовища, а другий – доступ до фізичних з'єднань і залежить від них.

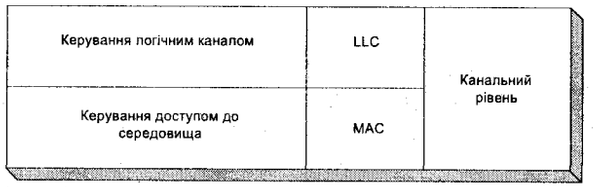


Рис. 6.1. Підрівні канального рівня.

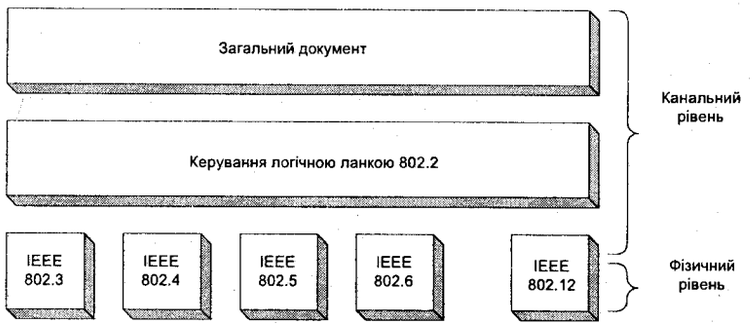


Рис. 6.2. Структура стандартів IEEE-802.

Велику роботу зі стандартизації протоколів веде Комітет 802 IEEE Міжнародного інституту інженерів-електриків та електроніків, що розробив кілька стандартів протоколів канального і фізичного рівнів (рис. 6.2).

У стандарті IEEE-802.1 відображені загальні теоретичні проблеми побудови локальної мережі та взаємодія з верхніми рівнями. Стандарт IEEE-802.2 визначає процедури обміну даними між системами на підрівні керування логічною ланкою LLC. Він є загальним для всіх типів фізичних з'єднань та методів доступу і не залежить від їхніх характеристик. Стандарти IEEE-802.3–802.12 визначають процедури доступу для різних методів доступу та передавальних середовищ і залежать від їхніх особливостей. Наприклад, IEEE-802.3 визначає процедури керування для МДКН/ВК (CSMA/CD), IEEE-802.4 – для маркерного методу доступу в моноканалі, IEEE-802.5 – для маркерного методу доступу в кільцевих мережах з ретрансляцією, IEEE-802.12 – для методу доступу з запитами пріоритету (DPP).

6.3. Стандартні реалізації багатопротокольних мереж на канальному рівні

На початку розвитку локальних мереж у кожній окремій мережі можна було передавати кадри тільки одного формату. З часом, коли комп'ютерні мережі стали достатньо складними і об'єднують значну кількість локальних мереж з різними форматами кадрів, виникла потреба реалізувати можливості одночасного передавання мережею кадрів різних форматів.

Для цього на кожному комп'ютері до адаптера додають спеціальну програму керування – драйвер, яка завантажується резидентно в пам'ять. Сьогодні є три підходи до організації взаємодії драйверів адаптерів з ПЗ, яке реалізує протокольні функції.

• У 1989 р. Microsoft та 3COM розробили специфікацію **NDIS** (Network Device Interface Specification), яка регламентує спосіб роботи мережевого адаптера з декількома протоколами. Сьогодні цю специфікацію використовують у таких системах, як LAN Manager, Windows for Workgroups, Windows 9x, Windows NT, Lantastic, Pathworks та ін. Реалізація NDIS є як для 16-бітових систем (NDIS 2.0), так і для 32-бітових (NDIS 3.0).

• Фірма Novell розробила та використовує **ODI** (Open Datalink Interface), що організований подібно до NDIS, але з іншим програмним інтерфейсом.

• Для мереж TCP/IP є компактні драйвери, розроблені фірмою FTP Software відповідно до специфікації **PDS** (Packet Driver Specification) .

Бібліографія та джерела

1. *Бараш Л.* Автосогласование в мультискоростных сетях Ethernet // Комп'ютерное обозрение. 1998. №34.
2. *Вейцман К.* Распределенные системы мини- и микро-ЭВМ / Пер. с англ. М.: Финансы и статистика, 1982.
3. *Девис Д., Барбер Д., Прайс У, Соломонидес С.* Вычислительные сети и сетевые протоколы. М.: Мир, 1982.
4. *Флинт Д.* Локальные сети ЭВМ: архитектура, принципы построения, реализация / Пер. с англ. М.: Финансы и статистика, 1986.

ДОДАТОК ДО РОЗДІЛУ 6

Д.6.1. Автоузгодження в мережах Ethernet

Розвиток технології Ethernet, поява вирішень, які підтримують значну швидкість передавання (Fast Ethernet, Gigabit Ethernet), створюють ситуації, коли в одній мережі одночасно використовують декілька різношвидкісних технологій Ethernet. Актуальним стає забезпечити взаємодію та одночасну роботу цих технологій. З погляду адміністратора мережі найзручніше було б, якби мережеві пристрої самі узгоджували швидкості та можливі технології передавання без ручного налагодження. Як один з можливих способів вирішити це завдання компанія National Semiconductor у 1994 р. запропонувала протокол та технологію *Nway Auto-Negotiation*. Сьогодні ця технологія прийнята IEEE 802.3 як попередній стандарт.

Партнерами операції узгодження є порт комутатора та адаптер. У цьому випадку автоузгодження забезпечується, якщо протокол узгодження підтримують обоє партнерів. Віддалений партнер позначають **LP** (Link Partner), а сам пристрій – **LD** (Local Device).

Принцип дії автоузгодження досить простий. Кожен партнер повідомляє іншому про технологію, яку він підтримує. Маючи інформацію про власні можливості та можливості партнера, LD обирає технологію обміну згідно з визначеними пріоритетами.

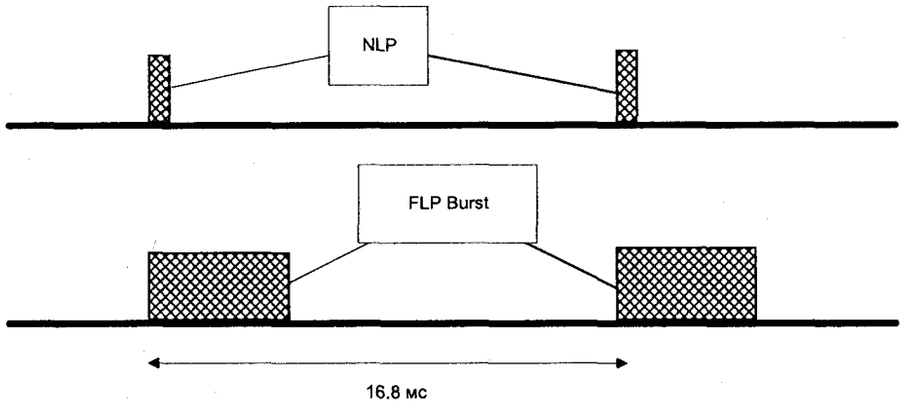


Рис. Д.6.1.1. Послідовність імпульсів.

Як же автоузгодження відбувається реально? Для реалізації протоколу автоузгодження використано таку властивість технології 10Base-T на фізичному рівні: коли інформація в каналі не передається, у канал періодично надходить короткий імпульс **NLP** (Normal Link Pulse) з періодом 16.8 мс. Це робиться для визначення працездатності приєднаного пристрою. Технологія автоузгодження пропонує замість одного короткого імпульсу NLP передавати цілу пачку (від 17 до 33) імпульсів NLP. Ця послідовність імпульсів одержала назву **FLP** (Fast Link Pulse Burst) (рис. Д.6.1.1).

Імпульси FLP Burst утворюють інформаційне слово **LCW** (Link Code Word). Його структура показана на рис. Д.6.1.2.

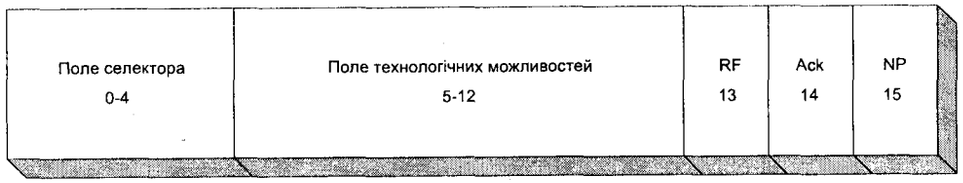
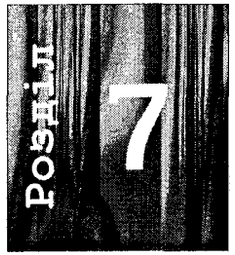


Рис. Д.6.1.2. Структура інформаційного слова.

Поле селектора визначає базову технологію. Наприклад, '00001' відповідає IEEE 802.3 (Ethernet). Поле технологічних можливостей визначає варіанти базової технології. Зокрема, '1' відповідає 100Base-TX Full Duplex, а '5' – 10Base-T. Отже, технологія автоузгодження підтримує 32 базові технології передавання та значну кількість їхніх варіантів. Біт RF (Remote Fault) повідомляє про помилку, а біт Ack підтверджує правильне приймання. Біт NP (Next Page) =1 інформує, що буде проведений обмін додатковими інформаційними словами, які можуть переносити як команди визначених форматів, так і довільні дані.

Перед початком обміну інформацією відбувається процедура синхронізації. LD надсилає LCW з бітом Ack=0. У відповідь LP відсилає копії LCW. Після коректного одержання трьох копій LD повторює декілька посилань з Ack=1, що підтверджує правильність приймання даних від LP. Як підтвердження, LP відсилає копії LCW з Ack=1. Після успішного приймання трьох копій переходять до процедури автоузгодження.

Технологія автоузгодження досить гнучка у використанні, передбачає розширення та появу в майбутньому нових технологій передавання.



ПРОТОКОЛИ КЕРУВАННЯ ДОСТУПОМ

Організація доступу до передавального середовища. Тактові системи. Централізоване керування. Методи опитування. Протокол MIL1553B. Метод доступу з використанням механізму провідникового "&". Методи конкурентного доступу. Метод доступу з контролем сигналу-носія та виявленням колізій. Маркерні методи доступу. Процедура реконфігурації. Методи доступу в мережах з ретрансляцією. Кільцеві ЛМ з уставленням регістру. Метод доступу з запитом пріоритету.

Розглянемо найнижчий підрівень канального рівня протоколу – підрівень керування доступом до фізичного середовища MAC. Головною функцією цього підрівня є забезпечення доступу окремих станцій до передавального середовища так, щоб перепускна здатність каналу зв'язку використовувалася ефективно.

Спосіб організації доступу станцій мережі до передавального середовища називається ***методом доступу.***

Є велика кількість різноманітних методів доступу. Вони різняться:

• *характером фізичного середовища* – методи доступу для моноканалу та мереж з ретрансляцією;

• *характером керування* – з централізованим та децентралізованим керуванням;

• *характером доступу* – конкурентні або з передаванням повноважень.

Розглянемо деякі методи доступу і відповідні протоколи.

7.1. Тактові системи

Основним принципом організації **тактових систем** (slotted systems) є циклічний розподіл усього часу передавання на однакові часові проміжки – **такти (слоти)**. За кожною станцією закріплено відповідний слот. Такий підхід започаткований ще в 50-х роках. Його широко використовували в системах телемеханіки. Якщо до мережі приєднано n абонентів, то кожен абонент має право передати свій кадр один раз на n слотів (рис. 7.1).

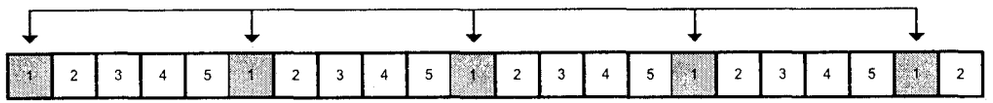


Рис. 7.1. Розподіл квантів часу в тактовій системі.

Така система подібна до конвеєрної лінії або поїзда, який постійно рухається. Тактові системи бувають синхронні та асинхронні. У синхронних системах є центральний таймер та лінія синхронізації. В асинхронних сигнали синхронізації передаються разом з інформацією.

Проте тактові системи мають такі недоліки:

• неефективність використання каналу. Внаслідок нерівномірності навантаження з'являється багато порожніх слотів. Вислідна швидкість передавання невисока;

• зі збільшенням кількості станцій ефективність мережі зменшується. Тому тактові системи не використовують з десятками або сотнями станцій.

Оцінимо перепускну здатність тактової системи на такому прикладі. Нехай m – кількість станцій. За один такт передається 256 інформаційних та 64 службові біти, отже, сумарна довжина кадру l=320 бітів. Нехай b – середня довжина повідомлення: b=1000 бітів, a – середня інтенсивність надходження повідомлень: a=2 повідомлення за 1 с. Якщо t – період кадру і t=0.4 с, то у кадр за секунду повинно поміститися tba=800 бітів. Для передавання 800 бітів треба 800/320 тактів. Кількість тактів на кадр заокруглюють до степеня двійки: n=4. Загальна кількість тактів у кадрі nm=80. Перепускну здатність системи можна обчислити як відношення загальної кількості бітів у кадрі до його періоду:

$$C=(nml)/t=102.4 \text{ Кбіт/с, де } n=f((tba)/l).$$

7.2. Метод опитування. Централізоване керування

Метод опитування використовують у шинних або ефірних мережах (polled networks). У цьому випадку один з приєднаних до мережі пристроїв вважається головним і називається *контролером мережі.* Він керує передаванням. Найпростіший варіант централізованого керування реалізується на базі циклічного опитування. Контролер по черзі опитує (надсилає кадри) приєднані пристрої. Вони відповідають, надсилаючи в мережу або інформацію, або спеціальний кадр, якщо інформації нема. Контролер після одержання кадру опитує наступний пристрій і т. д. У такій шині об'єднано два потоки: інформаційний та керування. Передавання інформації можна розділити на такти тривалістю

$$t_s=t_p+b/C,$$

де t_s – середня тривалість обслуговування; t_p – тривалість опитування; b – середня довжина кадру, який передається; C – перепускна здатність шини (рис. 7.2).

Нехай у мережі m станцій, а кожна машина передає за одиницю часу a повідомлень. Тоді інтенсивність потоку повідомлень становить am, а середній інтервал між надходженнями – $1/am$; $t_s \le 1/am$. Отже, перепускна здатність

$$C=(amb)/(1-amt_p).$$

Мережі з опитуванням, як звичайно, невеликі. Їх використовують у лабораторному, аерокосмічному, побутовому і військовому обладнанні.

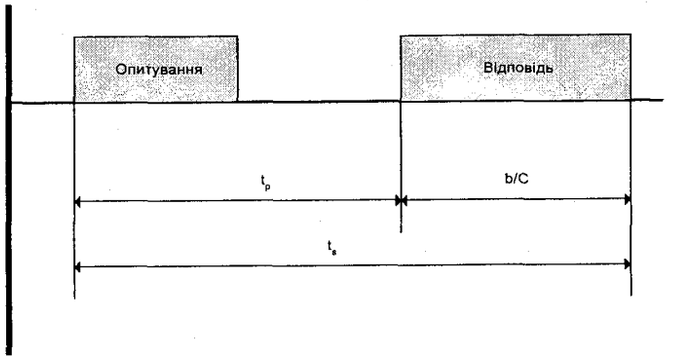


Рис. 7.2. Структура потоку в мережах з опитуванням.

Недоліки цих мереж такі.

• Наявність великого потоку керування, навіть якщо в абонента нема інформації для передавання. Однак водночас постійно контролюється працездатність пристроїв.

• Надійність мережі визначається надійністю контролера. Якщо він вийде з ладу, то вийде з ладу вся мережа.

• Мережа обмежена щодо кількості абонентів. Чим більше абонентів, тим більше потрібно часу для опитування, отже, тим менша перепускна здатність.

Прикладом мережі з опитуванням є мережа стандарту MIL 1553B.

7.3. Особливості функціонування мережі стандарту MIL 1553B

Стандарт мережі MIL 1553B розроблено для ВПС США як основу передавання даних у військових літальних апаратах. Пізніше його скопіювали у стандарт ГОСТВ 24.394-80 для радянських військових літаків. Мережа, згідно з цим стандартом, характеризується високою перепускною здатністю, надійністю, незначною чутливістю до завад. Бортова система забезпечує обмін даними між різними автономними підсистемами, що розміщені в різних частинах літака. Такі підсистеми призначені для розв'язування задач обчислювального типу, збирання та первинного опрацювання інформації від давачів. Відповідно до стандарту MIL 1553B бортові підсистеми, які називають терміналами, з'єднують за допомогою двопроводової інформаційної магістралі, виконаної у вигляді екранованої скрученої пари. Для підвищення надійності на борту можуть бути дві або більше резервних магістралей.

Станцію мережі приєднують за допомогою адаптера. Адаптер складається з розв'язувального трансформатора, приймача-передавача, генератора тактових імпульсів, шифратора-дешифратора. Шифратор-дешифратор виконує основні функції перетворення даних, а саме: кодування-декодування даних у коді Манчестер II, перетворення з паралельного коду в послідовний і навпаки, контроль достовірності прийнятого слова, декодування адреси термінала та

ін. Слова формує термінал. Використовуючи стандарт MIL 1553B, за допомогою магістрального інтерфейсу можна об'єднати до 31 термінала.

Передаванням даних керує одна з підсистем – контролер. Обмін даними відбувається асинхронно в напівдуплексному режимі. На початку слова є спеціальний синхронізаційний символ (рис. 7.6). У кінці слова є один розряд для перевірки на парність. Дані передаються в послідовному коді зі швидкістю 1 Мбіт/с і до 47 тисяч інформаційних слів за секунду. Довжина магістралі не перевищує 100 м. Ймовірність появи помилки під час передавання слова не більше 10^{-7}.

У випадку *передавання даних від контролера до термінала* контролер передає командне слово, в якому зазначено адресу термінала, вимогу виконати операцію приймання даних і кількість інформаційних слів. Далі відбувається передавання інформаційних слів. Потім контролер чекає від термінала слово стану, яке підтверджує, що збоїв нема (рис. 7.3).

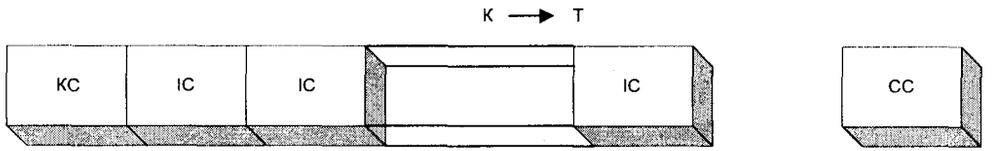


Рис. 7.3. Структура передавання даних від контролера до термінала.

Передавання даних від термінала до контролера відбувається так. Контролер ініціює обмін передаванням командного слова, у якому є вимога виконати операцію передавання даних, адреса термінала, кількість інформаційних слів. Термінал, який бере участь в обміні, відповідає контролеру словом стану, після чого починає передавати задану кількість інформаційних слів (рис. 7.4).

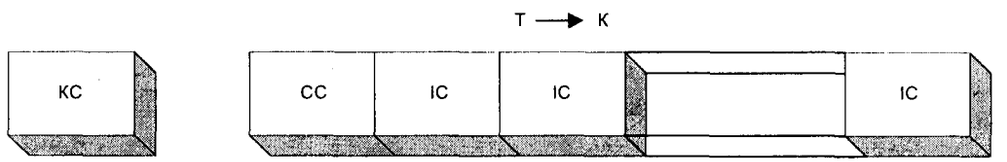


Рис. 7.4. Структура передавання даних від термінала до контролера.

У випадку *передавання даних між двома терміналами* контролер передає магістраллю два командні слова. У першому з них зазначено адресу термінала, який повинен прийняти дані, вимогу виконати операцію приймання, кількість інформаційних слів, у другому – адресу термінала, який передає дані, вимогу виконати операцію передавання, кількість інформаційних слів. Закінчується обмін тим, що термінал-приймач пересилає слово стану для контролера (рис. 7.5).

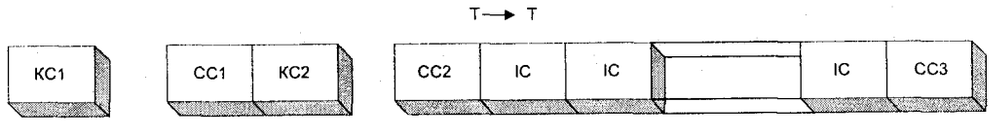


Рис. 7.5. Структура передавання даних між двома терміналами.

Можна також організувати *передавання даних усім терміналам відразу*. У цьому випадку контролер передає в магістраль слово з фіксованою адресою, яку розпізнають усі термінали.

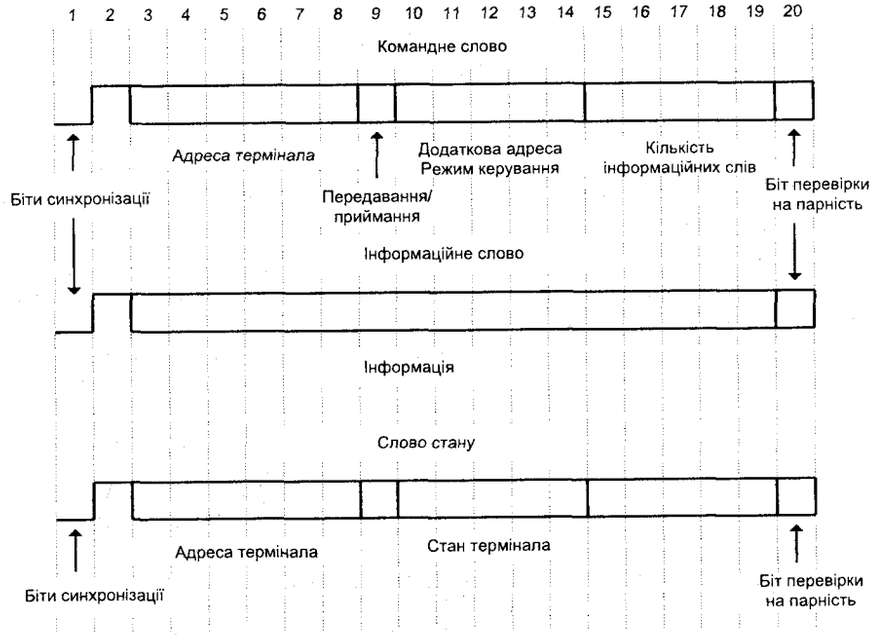


Рис. 7.6. Структура слів стандарту MIL 1553B.

Стандарт допускає передавання в одному повідомленні до 32 інформаційних слів, а також команд без інформаційних слів. Є три типи слів: командне, інформаційне, стану (рис. 7.6). У слові будь-якого типу є 20 розрядів: 16 інформаційних, 1 контрольний, 3 для синхронізації.

7.4. Метод доступу з використанням механізму провідникового "&". Малі локальні мережі I²C, D²B

Концепція мереж I²C, D²B розроблена фірмою Philips для різних потреб.

Мережа I²C була призначена для побудови нового типу телевізорів, якими керував комп'ютер. Тому її довжина становила до 10 м, швидкість передавання інформації – 7.5 Кбіт/с, якщо розмір кадру 2.5 байти, та 10.8 Кбіт/с, якщо розмір кадру 64 байти (рис. 7.7).

D²B (Digital Data Bus) – мережа більша. Вона обслуговує сукупність пристроїв. Максимальна її довжина становить 150 м, максимальна перепускна здатність – 8 Ксимв/с. До мережі можна приєднати до 50 станцій. D²B розроблена як побутова ЛМ (рис. 7.8). Вона добре захищена від електромагнітних завад. Аналогом D²B є мережа галузевого стандарту 4.239.001-85. Обидві мережі є шинами з розподіленим керуванням, де всі станції рівноправні. У мережі нема фіксованої швидкості передавання, вона автоматично адаптується до заданої швидкості (максимум –100 Кбіт/с.)

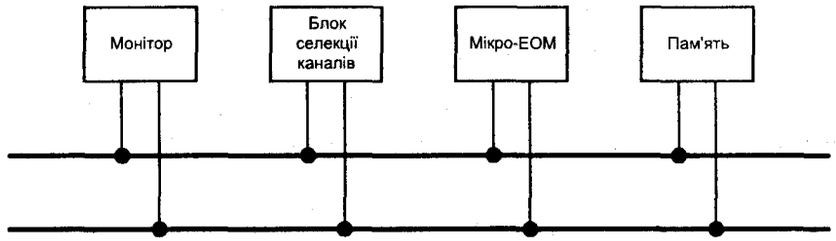


Рис. 7.7. Структура з'єднання пристроїв мережею I²C.

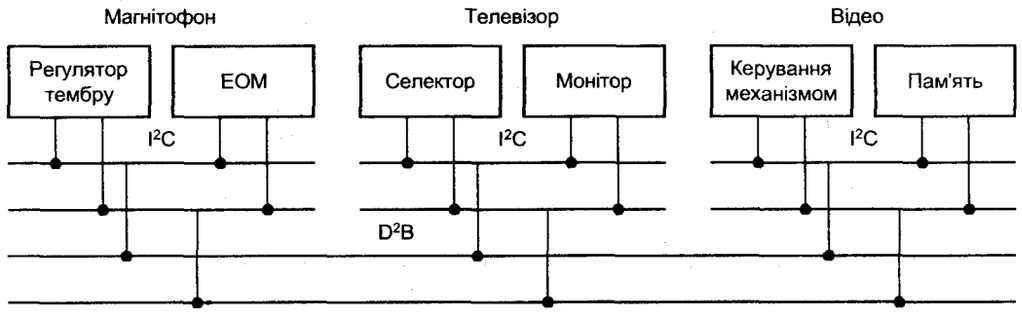


Рис. 7.8. Структура з'єднання пристроїв мережами I²C та D²B.

З метою уникнути колізій і забезпечити захоплення шини I²C тільки однією станцією використовують механізм провідникового "&". Він полягає в такому: якщо на всіх станціях вихідні транзистори закриті, то рівень сигналу на лінії буде високим; якщо ж хоча б один транзистор відкритий, то рівень сигналу буде низьким (рис. 7.9).

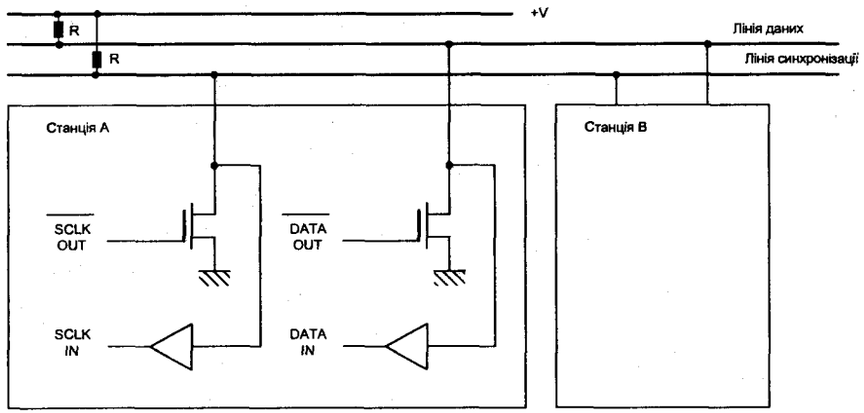


Рис. 7.9. Принцип провідникового "&".

Шина I²C має дві лінії: лінію даних та лінію синхронізації. Лінією синхронізації ідуть імпульси. Якщо на цій лінії рівень сигналу високий, то дані з лінії даних можна читати, якщо ж низький, – то їх можна змінювати (рис. 7.10, *а*).

Інформація в мережі передається побайтно. Початок передавання визначається зниженням рівня сигналу на лінії даних у випадку, якщо рівень сигналу на лінії синхронізації високий (рис. 7.10, *б*).

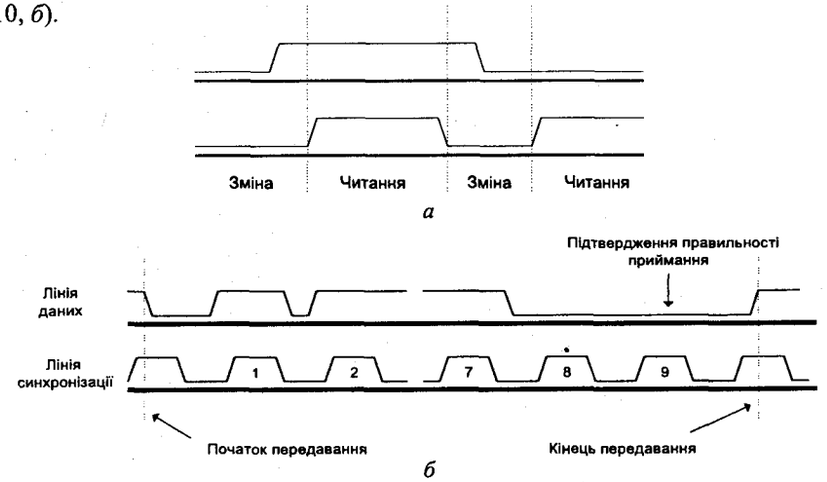


Рис. 7.10. Передавання одного біта (*а*) та одного байта (*б*) в мережі I²C.

Відсутність сигналу на лінії даних під час дев'ятого імпульсу синхронізації підтверджує правильне приймання. Перехід лінії даних на високий рівень сигналу при високому рівні сигналу на лінії синхронізації (після дев'ятого синхроімпульсу) означає кінець передавання. У кожний момент часу передавання виконує тільки одна станція. Вона синхронізує роботу всіх інших станцій та вибирає собі адресата (перше зниження рівня сигналу в лінії синхронізації синхронізує всі синхрогенератори) (рис. 7.11).

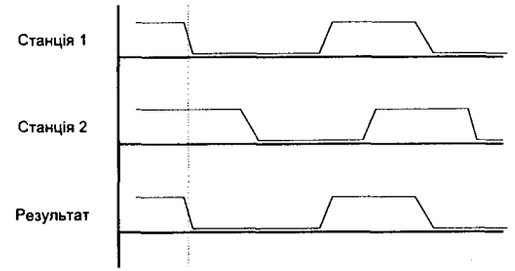


Рис. 7.11. Синхронізація синхрогенераторів.

Пристрій, який найдовше генерує низький рівень сигналу, буде визначати період синхросигналу. Якщо дві станції почнуть передавати інформацію одночасно, то спрацює процедура арбітражу (рис. 7.12).

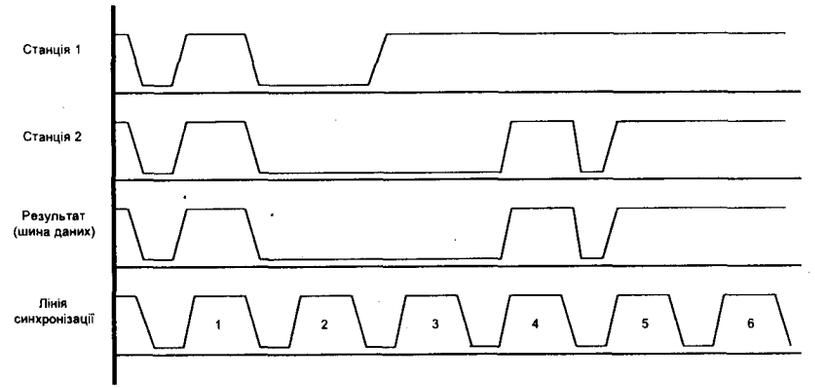


Рис. 7.12. Процедура арбітражу.

Розглянемо цю ситуацію детальніше. Нехай дві станції передають інформацію одночасно. Під час першого синхроімпульсу вони мають високий рівень сигналу. Конфлікту немає. Під час другого синхроімпульсу вони мають низький рівень сигналу. Конфлікту також немає. Однак під час третього імпульсу станція 1 видає високий рівень сигналу, а станція 2 – низький. Виникає конфлікт. Лінія даних у результаті матиме низький рівень сигналу, і станція 1 помітить різницю, тому виставить високий рівень, який у подальшому не буде впливати на передавання, і відмовиться від передавання.

Структура кадру в мережі I²C показана на рис. 7.13, тут *R/W* – це біт-ознака, яка визначає, що повинна робити станція-одержувач після приймання кадру – передавати чи приймати інформацію, біт *A* повідомляє про одержання даних приймачем.

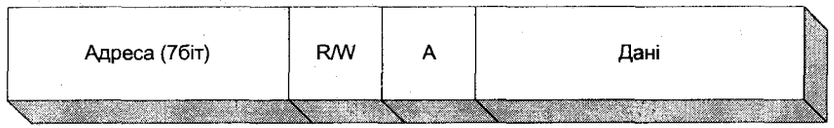


Рис. 7.13. Структура кадру в мережі I²C.

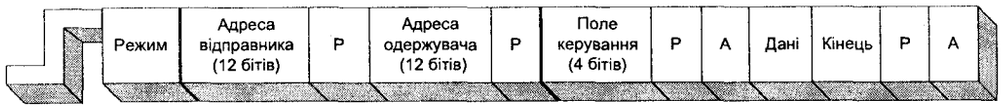


Рис. 7.14. Структура кадру мережі D²B: *P* – біт парності; *A* – біт підтвердження приймання кадру.

Структура кадру в мережі D²B зображена на рис.7.14. Як бачимо, кадр починається стартовим бітом, що має спеціальну форму. Біти 1–3 є бітами режиму і задають швидкісний режим обміну. Після цього передаються 12 бітів адреси головного пристрою, захищені бітом парності *P*. Далі – 12 бітів адреси підпорядкованого пристрою, також захищені *P* та *A*. Під час передавання бітів режиму відбувається арбітраж щодо швидкості. Продовжують передавати пристрої з однією, найменшою швидкістю. Після передавання адреси головного пристрою в мережі залишиться головний пристрій з найменшою адресою. Підпорядкований пристрій, якщо він готовий до приймання або передавання, виробляє біт *A*. Далі є контрольне поле з чотирьох бітів. Воно захищене бітом парності і вимагає від приймача підтвердження можливості виконання заданих у ньому режимів. Потім передаються *n* байтів даних. Після кожного байта передається біт підтвердження та парності. Закінчується кадр бітом кінця даних та бітом підтвердження.

7.5. Методи конкурентного доступу

У мережах з централізованим керуванням та в маркерних мережах станція повинна чекати, щоб одержати дозвіл на передавання. Крім того, багато часу витрачається на передавання службової інформації. Розробники **методів конкурентного доступу** вирішили дати змогу будь-якій станції передавати інформацію тоді, коли їй буде потрібно, а також спробували мінімізувати наслідки неминучих у такому випадку колізій. Вони ставили собі за мету забезпечити мінімум службової інформації та максимальну швидкість доступу до каналу зв'язку.

Методи конкурентного доступу (їх ще називають методами доступу з суперництвом) діють, як звичайно, у моноканалі. Вперше такий підхід застосовано під час розробки мережі для університету штату Гавайї (система **ALOHA**). У цій системі середовищем передавання був радіоканал. Кожна станція, яка мала кадр для передавання, передавала його. Однак у випадку, коли передавачів, що працювали одночасно, було багато, то деякі станції передавали кадри також одночасно, отже передавання накладалися. Виникали колізії. Тому мережа ALOHA була ефективною тільки тоді, коли інтенсивність надходження кадрів для передавання була малою. Реальна перепускна здатність мережі досягала 19% від максимальної.

Найбільшого поширення методи конкурентного доступу набули у шинних мережах. Власне в них було вперше використано принцип 'слухай перш ніж говорити' – **контроль сигналу-носія,** тобто прослуховування каналу. У таких мережах станція постійно прослуховує канал. Якщо канал вільний, станція починає передавання, якщо ж зайнятий – чекає. Цей метод називається ***методом доступу з контролем сигналу-носія (МДКН)*** (*Carrier Sense Multiple Access (CSMA)*). Однак виявилося, що й тут також можливі колізії. Чому ж вони виникають?

Час поширення сигналу мережею скінченний. Якщо одна станція почала передавання, а до другої сигнал ще не дійшов, то вона теж може почати передавання. Тоді й виникає колізія (рис. 7.15).

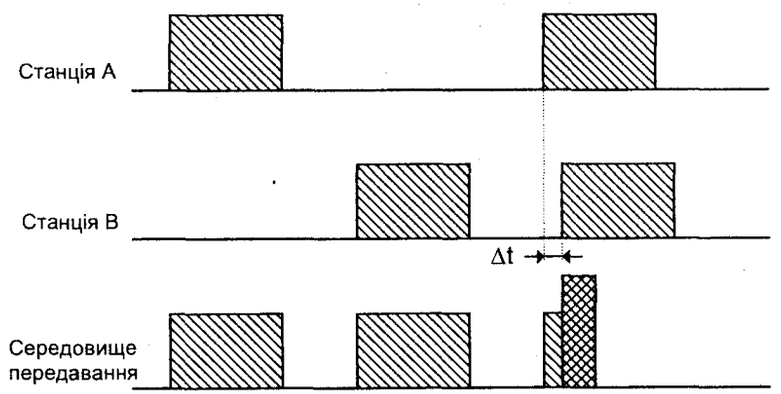


Рис. 7.15. Виникнення колізії.

Нехай $\Delta t_{ij}=t_i-t_j$ – різниця часу між початками передавання кадрів станціями *i* та *j*; τ_{ij} – час поширення сигналу від станції *i* до станції *j*. Тоді умову виникнення колізії між передаваннями станцій *i* та *j* можна записати так:

$$\Delta t_{ij} \le \tau_{ij},$$

а умову виникнення колізії в мережі – так:

$$\exists (i,j)\ (\Delta t_{ij} \le \tau_{ij}).$$

Для ефективного використання каналу треба зменшити тривалість колізії. Водночас треба дати час усім станціям зафіксувати наявність колізії. Тому станції, які увійшли у колізію, передають шумову послідовність протягом часу 2τ, причому

$$\tau = \max_{i,j} \tau_{i,j}.$$

Станції, які не передали свої кадри внаслідок колізії, знову пробу.ють передати інформацію.

Ще одним джерелом виникнення колізій є інертність самого пристрою, що виконує протокольні функції.

Максимальна ефективність цього методу становить 53%.

Найбільшої ефективності (93%) вдалося досягти за допомогою методу доступу МДКН/ВК (Carrier Sense Multiple Access with Collision Detection (CSMA/CD)). У цьому випадку час очікування на передавання після вивільнення каналу вибирається випадково з використанням давача випадкових чисел. Таким чином зменшується ймовірність взаємного блокування повторних передавань станцій. Алгоритм роботи за МДКН/ВК показаний на рис. 7.16.

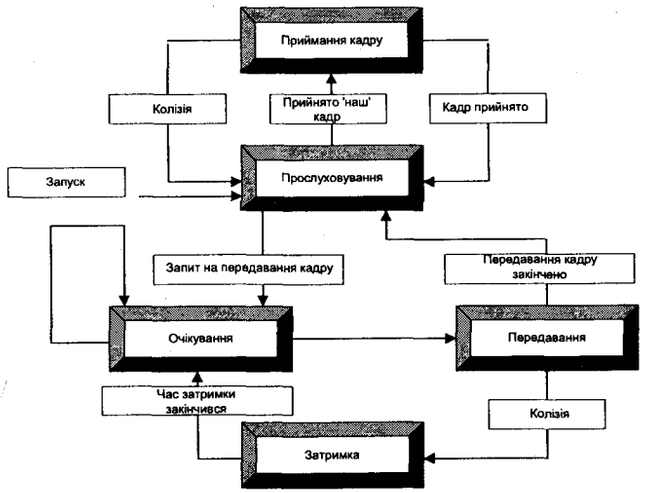


Рис. 7.16. Алгоритм функціонування МДКН/ВК.

Станція постійно прослуховує середовище передавання й аналізує адреси всіх кадрів, що передаються. Якщо кадр адресовано цій станції, то вона його приймає, а потім знову прослуховує середовище. У випадку, коли від протоколу верхнього рівня надішов запит на передавання кадру, то станція його передає відразу, якщо середовище передавання вільне, або чекає, доки воно вивільниться. Якщо передавання закінчилося нормально, то станція прослуховує середовище. Якщо ж виявлена колізія, то станція визначає випадковий інтервал затримки і знову очікує вивільнення середовища.

Перевагою МДКН/ВК є висока ефективність, а також те, що тут немає службової інформації. Недоліки методу: мережа з МДКН/ВК ефективна, якщо навантаження мале; зі збільшенням навантаження вплив колізій збільшується. У мережі з МДКН/ВК також не можна гарантувати тривалості передавання кадру.

Оцінимо ефективність цього методу доступу. У системах з конкуренцією ймовірність того, що за час τ лише одна станція захопить шину, така:

$$A = (1-1/Q)^{Q-1},$$

де Q – кількість станцій у черзі на передавання кадрів. Тоді ефективність шини можна обчислити за формулою

$$E = \frac{P/C}{P/C + W\tau},$$

де P – довжина кадру, біт; C – максимальна перепускна здатність шини; W – середня кількість інтервалів часу, які минули на етапі конкуренції:

$$W = (1-1/A).$$

Отже, ефективність МДКН/ВК залежить від часу τ. Крім того, чим більша довжина шини або чим менша швидкість поширення сигналу, тим менша ефективність шини. Прикладом мережі з МДКН/ВК є ЛМ Ethernet.

7.6. Маркерні методи доступу

Маркерний метод доступу (token passing) полягає в тому, що в мережу вводять спеціальний кадр – маркер, який переходить від станції до станції почергово. Як звичайно, це залежить від адреси станції (за зростанням або спаданням її номера). Остання станція передає маркер першій і так виникає логічне кільце (рис. 7.17). Станція, яка в конкретний момент часу має маркер, одержує право на передавання.

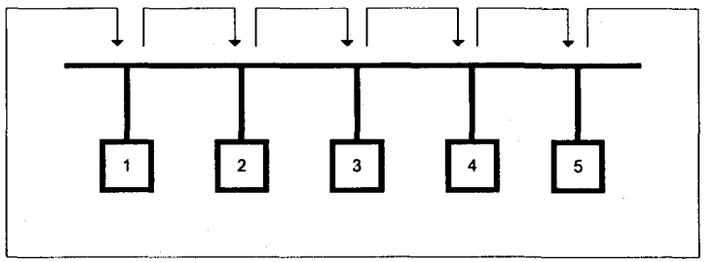


Рис. 7.17. Логічне кільце.

Маркерний метод доступу означено для мереж шинної, кільцевої, зірко- та деревоподібної конфігурацій, моноканалу і мереж з ретрансляцією. Його використовують у мережах Arcnet, Domain, Token Ring, Ringnet та ін. Стандартизовано маркерні методи доступу в IEEE-802.4-5.

Розглянемо спочатку шину з передаванням маркера.

Маркерний доступ у шинній мережі. Алгоритм роботи шини з маркерним доступом показано на рис. 7.18. Станція, що є в логічному кільці, постійно прослуховує шину і приймає адресований їй кадр. Якщо цей кадр маркерний, то станція у випадку наявності інформації спочатку передає інформаційний кадр, а потім – маркерний, якщо ж інформації на передавання нема, то лише маркерний.

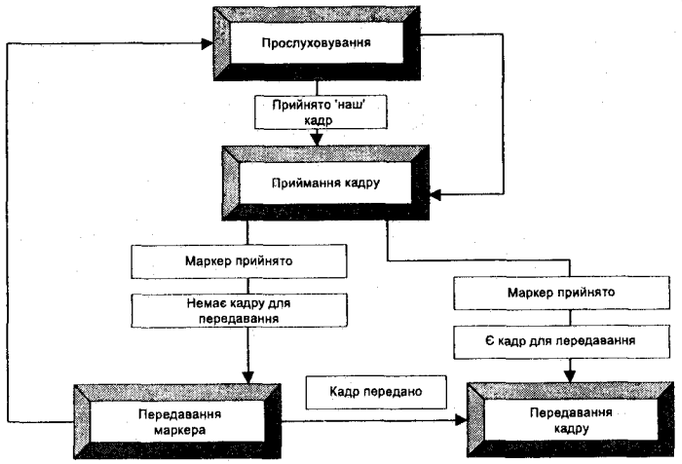


Рис. 7.18. Алгоритм маркерного методу доступу.

Структура маркерного кадру зображена на рис. 7.19.

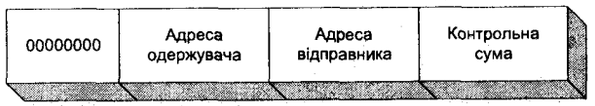


Рис. 7.19. Структура маркерного кадру.

Використання логічного, а не фізичного кільця передбачає реалізацію таких функцій:

- від'єднання станції від логічного кільця;
- приєднання станції до логічного кільця;
- зміна параметрів алгоритму (наприклад, максимальний час, протягом якого станція може утримувати маркер);
- втрата та дублювання маркерів.

Будь-яка станція може від'єднатися від логічного кільця в той момент, коли має маркер. Для цього вона надсилає попередній у логічному кільці станції кадр *Налагодження наступного вузла* (рис. 7.20), а опісля від'єднується.

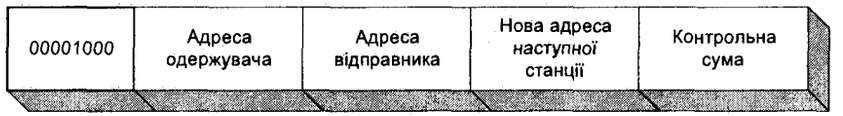


Рис. 7.20. Структура кадру *Налагодження наступного вузла*.

Зворотна операція, тобто приєднання, може відбуватися кількома способами. Опишемо два з них.

Перший спосіб такий. Кожна станція через *n* тактів запускає процедуру суперництва. На початку процедури вона передає кадр *Шукання наступного вузла*, в якому є вікно (рис.7.21).

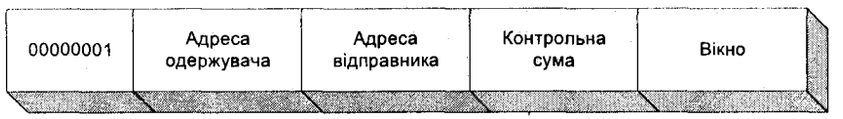


Рис. 7.21. Структура кадру *Шукання наступного вузла*.

Станції, які бажають приєднатися до кільця, надсилають у вікні кадр *Налагодження наступного вузла.*

Другий спосіб – це **процедура реконфігурації**. Станція, якій потрібно приєднатися до кільця, починає передавати збійну послідовність, що призведе до втрати маркера і реконфігурації мережі (рис. 7.22). Після збою всі станції перебувають у стані бездіяльності. Станція збуджується, коли закінчився тайм-аут або одержано маркер. Тривалість тайм-ауту пропорційна до номера станції, тому станція з найменшим номером збудиться першою. Така станція є у стані опитування, тобто вона передає маркерні пакети станції з наступною за порядком адресою. Якщо через деякий час відповіді нема, маркер знову передається станції з наступною адресою і т.д. Попередня станція сприймає початок передавання маркерів як відповідь і переходить у режим нормальної роботи. Так триває доти, доки станція з найбільшим номером не перешле маркер першій станції, яка вже перебуває у стані нормальної роботи. Після цього маркер є у першої станції, і розпочинається нормальна робота мережі.

Мережа з ретрансляцією і передаванням маркера. Головна відмінність кільцевої мережі від шини-моноканалу полягає в тому, що у станціях кільцевої мережі інформацію приймають, аналізують і далі передають на сусідню станцію (рис. 7.23). Завдяки проміжному прийманню та передаванню кадрів у мережі з ретрансляцією сигнал у проміжній станції можна

підсилити. Тому у кільцевих мережах довжина з'єднань не обмежена, на відміну від моноканальних мереж.

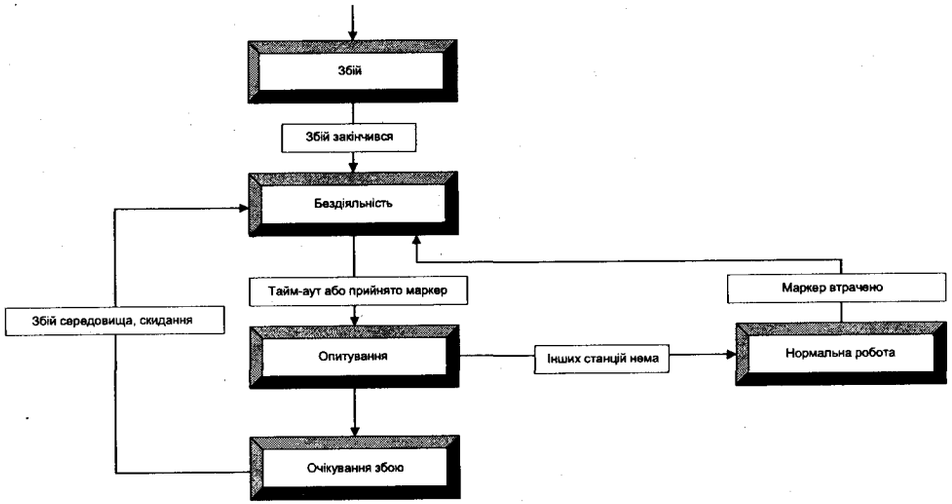


Рис. 7.22. Процедура реконфігурації.

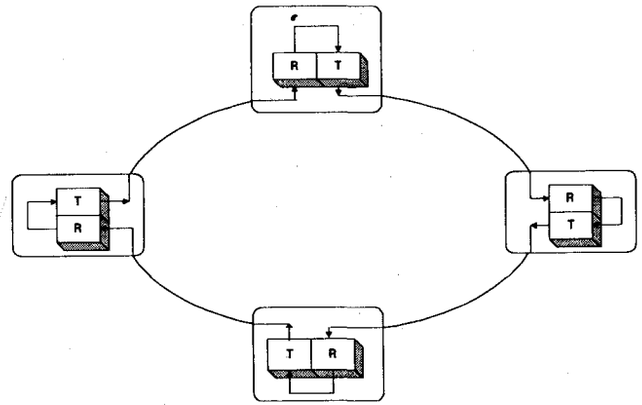


Рис. 7.23. Кільцева мережа.

У кільцевій мережі маркер не має поля адреси. Натомість він може бути у двох станах – вільному та зайнятому. Якщо станції мережі не мають інформаційних кадрів, то по мережі проходить вільний маркер. Станція, яка має інформацію для передавання, чекає вільного маркера. Коли

цей маркер надходить до неї, станція змінює його стан на зайнятий і додає ще інформаційний кадр. Зайнятий маркер переміщується кільцем. Змінити його стан на вільний може тільки та станція, яка його зайняла. Інформаційний кадр, доданий до маркера, має у заголовку адресу призначення, яку станції, приймаючи та передаючи цей кадр, аналізують. Станція, якій цей кадр адресовано, передає його на вищий рівень, а крім того, повторює далі по мережі. Таким чином маркер з інформаційним кадром через деякий час знову потрапляє на станцію, яка його зайняла. У цьому випадку станція забирає кадр з мережі і вивільняє маркер.

Якщо в шинній мережі якась станція від'єднується, то шина продовжує працювати. У кільцевий мережі від'єднання однієї станції виводить з ладу цілу мережу, тому потрібно вжити спеціальних заходів щодо збільшення її надійності.

Зокрема, одним із способів зробити кільцеві мережі надійнішими є зірково-кільцева топологія або встановлення спеціальних реле, що від'єднують станцію (рис. 7.24).

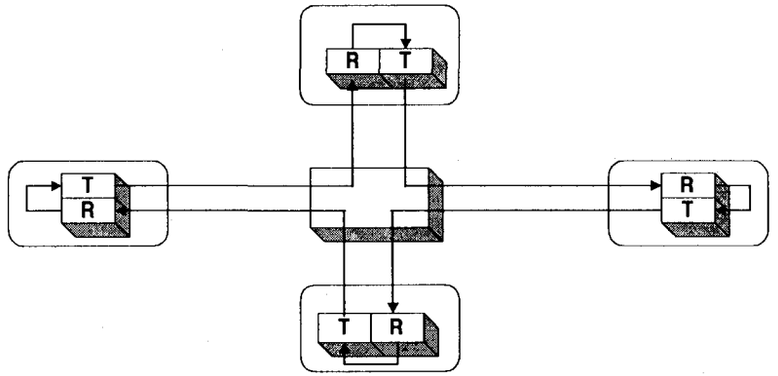


Рис. 7.24. Зірково-кільцева топологія.

Іншим способом може бути шунтування (рис. 7.25) або введення другого, рівнобіжного кільця (рис. 7.26).

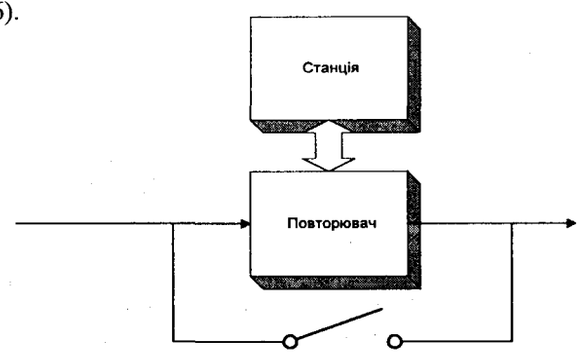


Рис. 7.25. Шунтування станції.

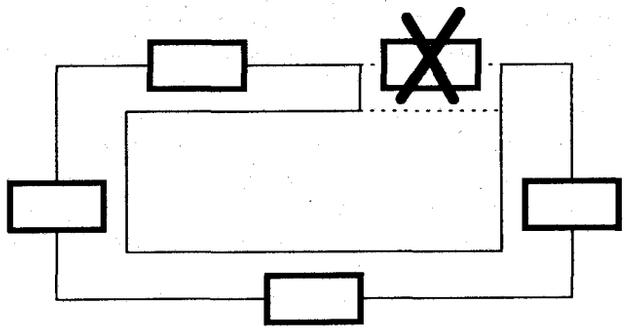


Рис. 7.26. Використання рівнобіжного кільця.

7.7. Кільцеві ЛМ з уставлянням регістра

Кільцеві ЛМ **з уставлянням регістра** (register insertion ring) розробив Е.Р.Харнер з університету штату Огайо (США) для мережі DLCN. Особливість цієї мережі полягає в новій конструкції передавача станції (рис. 7.27).

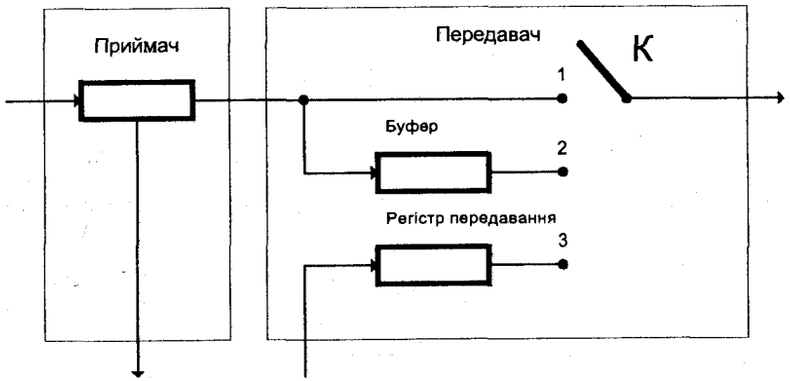


Рис. 7.27. Структурна схема станції ЛМ з уставлянням регістра.

Станція має приймач і передавач. Приймач аналізує адресу кадру, що надійшов. Якщо кадр адресовано станції, він передається для опрацювання протоколам верхніх рівнів та вилучається з кільця. В іншому випадку кадр потрапляє на вхід передавача.

Алгоритм роботи передавача такий. Якщо даних для передавання нема, а буфер порожній, то ключ *K* перебуває в положенні *1*. Відбувається повторення кадрів, що надходять з приймача. Якщо з'явилися кадри для передавання, вони записуються в регістр передавання

(РП). Коли передавання кадру в каналі закінчилося і якщо РП не порожній, то ключ *K* перемикається у положення *3* – відбувається передавання кадрів з РП. Кадри, що надходять тим часом з каналу, накопичуються в буфері. Якщо передавання з РП закінчилося або буфер близький до заповнення, передавання кадрів станції припиняється, ключ перемикається в положення *2* – передаються кадри з буфера. Потім ключ знову набуде положення *1*. Щоб не було великої затримки кадрів, ємність регістрів буфера та РП треба обмежити. Для мінімізації тривалості відповіді кадри повинні бути короткими. Оскільки кадри з кільця вилучає станція-адресат, то ефективність використання каналу в такій мережі досить висока. Метод доступу з уставлянням регістра застосовано в мережі 'Естафета'.

Наведемо деякі формули для оцінки ефективності цього методу доступу. Середня тривалість перебування передавача в станах *1*, *2*, *3* можна обчислити такими формулами:

$$t_1=t_1^1=\gamma/\lambda-\lambda_T\gamma(1/\mu+\lambda/\mu^2)(1/\mu+\lambda_T/\mu^2);$$

$$t_2=t_2^0=\lambda_T\gamma(1/\mu+\lambda/\mu^2)(1/\mu+\lambda_T/\mu^2);$$

$$t_3=t_3^0=\gamma(1/\mu+\lambda/\mu^2),$$

де γ – ємність регістра РП; λ – інтенсивність потоку кадрів, які генерує станція; λ_T – інтенсивність транзитного потоку; μ – інтенсивність обслуговування.

Тривалість чекання кадру цієї станції на передавання

$$T_{oc}=\frac{\gamma\left(1+\mu^2+\lambda^2\right)}{2\lambda\mu(\mu+\lambda)}.$$

Середня тривалість чекання для транзитного кадру

$$T_{ot}=\frac{n_1/\mu\left(t_2+t_3\right)+t_3^2}{2\left(t_1+t_2+t_3\right)}.$$

Потрібна ємність n_1 буфера

$$n_1=\lambda_T\gamma(1/m+1/m^2).$$

7.8. Метод доступу з запитом пріоритету

Метод доступу з запитом пріоритету (Demand Priority Protocol (DPP)) розроблено фірмами HP та AT&T і стандартизовано IEEE в 1995 р. (стандарт IEEE-802.12). Його реалізовано в мережі 100VG-Anylan.

Ця мережа має топологію розгалуженого дерева (рис. 7.28).

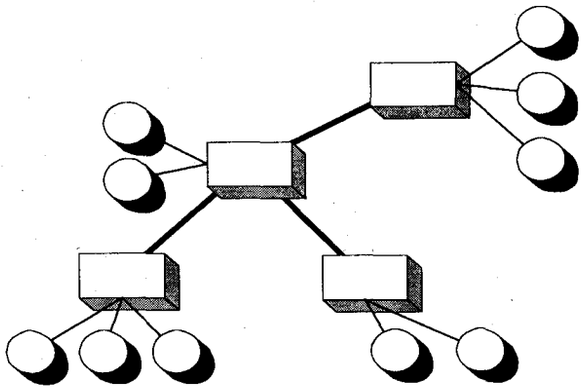


Рис. 7.28. Топологічна структура мережі з DPP.

Центром кожної зірки є комутатор, який має вхідні та вихідні порти. До вихідних портів приєднані пристрої нижніх рівнів дерева, які називаються вузлами. Вхідний порт приєднано до комутатора верхнього рівня. Комутатор періодично опитує свої вихідні порти про наявність інформації для передавання. Запит на передавання, який надходить від вузла, має рівень пріоритету. Нормальний пріоритет використовують для передавання файлів, а високий – відеоінформації, мовлення тощо. Якщо приєднаний до комутатора пристрій має кадр найвищого пріоритету, він передає його комутатору. Той аналізує адресну інформацію і передає кадр іншому вузлу або комутатору верхнього рівня.

Перевагою методу доступу з запитом пріоритету є відсутність колізій, можливість передавання різних типів даних (файлів, відео, аудіо), висока ефективність використання смуги пропускання при високих навантаженнях (95%).

Бібліографія та джерела

1. *Вейцман К.* Распределенные системы мини- и микро-ЭВМ / Пер. с англ. М.: Финансы и статистика, 1982.
2. *Флинт Д.* Локальные сети ЭВМ: архитектура, принципы построения, реализация / Пер. с англ. М.: Финансы и статистика, 1986.
3. *Халсалл Ф.* Передача данных, сети компьютеров и взаимосвязь открытых систем. М.:Радио и связь, 1995.
4. *Хаусли Т.* Системы передачи и телеобработки данных. М.:Радио и связь, 1994.

ПРОТОКОЛИ КЕРУВАННЯ ЛОГІЧНИМ КАНАЛОМ

Розділ 8

Головні функції керування логічною ланкою. Протокол BSC. Особливості модемних протоколів. Протоколи Xmodem, Xmodem-CRC, Ymodem, Zmodem. Протокол HDLC. Послідовність фаз. Формат поля керування кадру. Головні команди. Фаза Логічне роз'єднання. Робота у фазі Ініціалізація. Фаза Налагодження сполучення. Робота у фазі Передавання інформації. Стани передавання, зайнято, зупинка, блокування, неприймання, часова витримка. Фаза Завершення сполучення.

Вищим підрівнем канального рівня протоколу взаємодії відкритих систем є LLC-підрівень керування логічною ланкою передавання (логічним каналом). Його функція – забезпечити правильне передавання даних між двома станціями (відправником інформації та її одержувачем) для довільного фізичного середовища передавання. У цьому випадку між об'єктами канального рівня налагоджується *логічний канал* (рис. 8.1). Увесь сервіс передавання забезпечує MAC-підрівень.

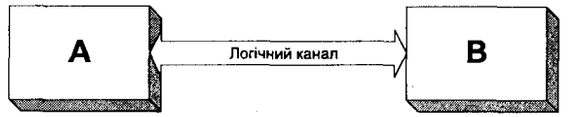


Рис. 8.1. Логічний канал.

Розглянемо приклади протоколів керування логічним каналом та функцій, які вони виконують, а саме: протоколи **BSC** (Byte Sequence Control), модемні протоколи та протокол **HDLC** (High-level Data Link Control).

8.1. Керування логічним каналом протоколу BSC

Протокол BSC розроблений фірмою IBM. Для керування та передавання цей протокол використовує символи стандартного коду ASCII. Передавання даних синхронне, напівдуплексне.

Кадри бувають інформаційними та керування. Кадри керування повідомляють про початок та кінець сеансу, помилки під час передавання; інформаційні кадри переносять повідомлення. Символи керування коду ASCII, що використовуються у кадрах, такі:

SOH	1		ACK	6	^F
STX	2	^B	DLE	16	^P
ETX	3	^C	NAK	21	^U
EOT	4	^D	SYN	22	^V
ENQ	5	^E	ETB	23	^W

Структура кадрів протоколу BSC показана на рис. 8.2. Як бачимо, кожен кадр починається з двох символів SYN. Крім того, є такі символи:

STX (Start of Text) – передує основі кадру;

SOH (Start of Header) – передує заголовку кадру;

ETX (End of Text) – є після закінчення кадру;

ETB (End of Text Block) – є після закінчення заголовка або основи кадру.

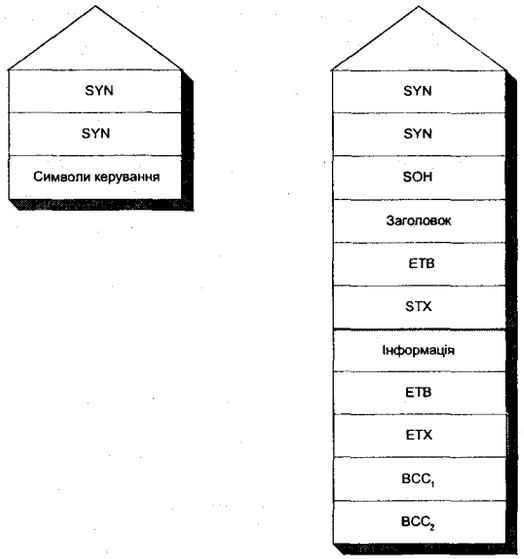


Рис. 8.2. Формати кадрів протоколу BSC.

Символи керування кадрів

ENQ (Enquiry) – запит на сеанс зв'язку або повторне передавання, якщо була помилка або кадр не надійшов.

ACK 0/1 (Acknowledgement) – символ підтвердження приймання та готовності до приймання наступного кадру.

ACK – символ підтвердження, але приймальна станція тимчасово не готова до приймання.

NAK (Negative Acknowledgement) – кадр має помилку і його треба передати ще раз.

RVI – переданий кадр був правильним, однак потрібно припинити передавання.

EOT (End of Text) – кінець сеансу зв'язку.

TTD – немає інформації для передавання. Прошу підтримувати сеанс зв'язку.

Два байти BCC_1 та BCC_2 є контрольними. Всі байти кадру додаються як арифметичні числа, сума ділиться на константу, залишок від ділення записується у контрольні байти. На приймальному кінці процедура обчислення повторюється.

Сеанс зв'язку складається з таких фаз:

- приєднання каналу (наприклад, набирання телефонного номера);
- запит на передавання;
- передавання кадрів;
- закінчення передавання;
- від'єднання каналу.

Приклади послідовності кадрів у випадку правильного та неправильного передавання показані на рис. 8.3.

Види інформаційних кодів, які надходять у канал, не обмежені (вимога прозорості), і серед них можуть бути службові символи протоколу BSC, що утруднить роботу програм керування. Щоб вирішити цю проблему, ввели спеціальний символ **DLE** (Data Link Escape). Його ставлять перед кожним символом керування в заголовку, кінці й основній частині. Цей процес називається **процедурою вставляння байтів** (bytestuffing). Після цього в головній частині перед символами керування ставлять ще по одному DLE.

Протокол BSC використовують для передавання даних між безпосередньо сполученими ЕОМ.

8.2. Протоколи модемів

Подібною до протоколу BSC є група протоколів передавання файлів за допомогою модема. Як і BSC, ці протоколи використовують символи керування коду ASCII. Головна мета цих протоколів – забезпечити передавання даних ненадійною ланкою передавання. Кожен кадр у них має фіксовану довжину та захищений контрольною сумою. Різні протоколи надають різний сервіс передавання. Складніші з них забезпечують захист сполучення від помилок, засвідчення сполучення, перевірку пароля.

До протоколів без захисту від помилок належать **Xmodem**, **Xmodem-CRC**, **Xmodem-1k**, **Ymodem**, **Kermit**. Протоколами, що реалізують захист від помилок, є **Ymodem-g**, **Zmodem**. Схарактеризуємо їх детальніше.

- **Xmodem** – один з перших модемних протоколів. Його розробив у 1977 р. В. Христенсен. Принцип роботи Xmodem такий (рис. 8.4).

Приймач постійно передає в канал символ NAK. Передавач, прийнявши цей символ з каналу, починає передавання: надсилає в канал символ SOH, два номери інформаційного блоку (номер та його двійкове доповнення), блок інформації, що має фіксовану довжину 128 байт, та байт контрольної суми. Останній формується як залишок від ділення суми всіх байтів блоку на 255. Контрольну суму повторно обчислює приймач. Якщо передане та обчислене значення не збігаються, то приймач передає в канал символ NAK, у протилежному випадку – ACK. Завершується передавання подвійним надсиланням символу EOT.

Відсоток виявлення помилок протоколом Xmodem досить значний (99.6%). Однак цей протокол має і суттєві недоліки: малу швидкодію, великий обсяг службової інформації.

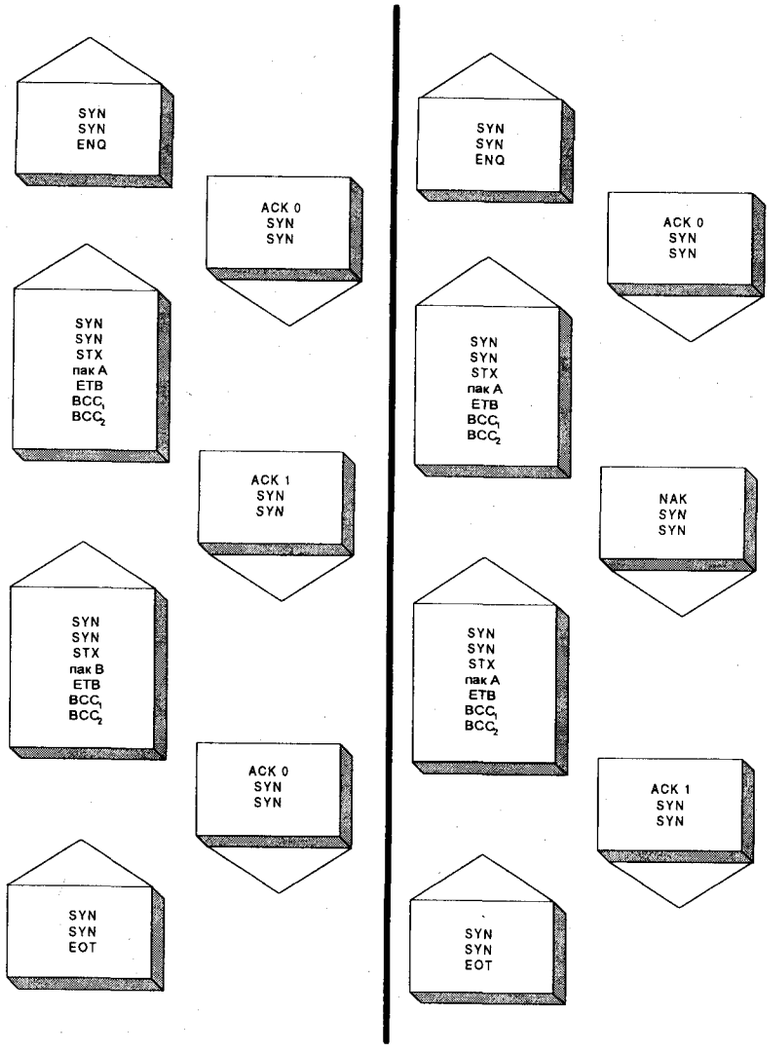


Рис. 8.3. Послідовність передавання кадрів протоколу BSC.

• **Xmodem-CRC** є модифікацією протоколу Xmodem. Кожен кадр у ньому замість одного має два контрольні байти. Протокол виявляє всі поодинокі, подвійні та непарні помилки, а також усі пакети помилок довжиною до 16 знаків. На початку передавання замість NAK приймач передає символ C. Якщо після трьох C відповіді не одержано, приймач починає роботу за Xmodem.

• **Xmodem-1k** – це модифікація протоколу Xmodem-CRC. Довжина інформаційного блоку в ньому збільшена до 1024 байтів. Кількість службової інформації зменшена. У системах з розподілом часу зменшується вплив затримок.

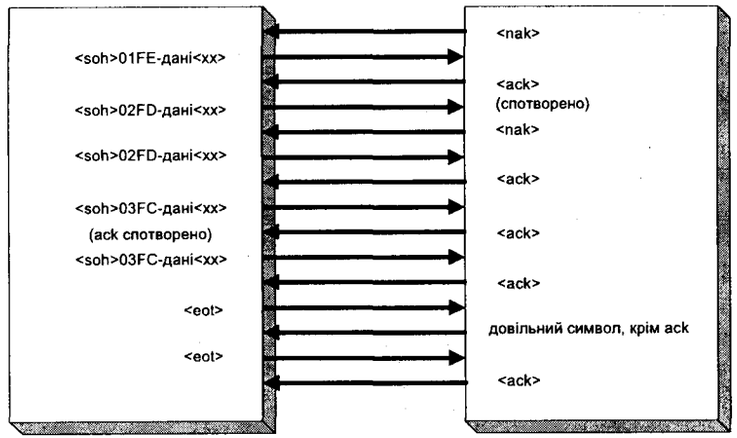


Рис. 8.4. Послідовність передавання кадрів протоколу Xmodem.

• **Ymodem** є протоколом Xmodem-CRC з додатковою реалізацією групового передавання файлів. Ім'я файлу та шлях до нього передаються в нульовому інформаційному блоці. В кінці кожного файлу передається до десяти разів символ EOT. Кінець сеансу позначається нульовим (порожнім) іменем шляху. Протокол використовують в операційних системах CP/M, RZ/SZ (Unix), пакеті MTEZ.

• **Ymodem-g** застосовують у високошвидкісних модемах та для захищених від помилок каналів. Передавання цим протоколом ініціює символ G. Передавач, який одержав G, відразу розпочинає передавання на найбільшій можливій швидкості. Швидкістю передавання керує протокол XON/XOFF.

Протокол XON/XOFF використовують так: якщо приймач не готовий до роботи, то він надає символ XOFF; тоді передавач тимчасово припиняє передавання, доки не отримає символ XON.

Виявивши помилку, приймач передає багато символів CAN. Підтверджує приймання файлу символ ACK. Протокол не захищає від помилок у каналі, у випадку їх виявлення передавання файлу припиняється.

• **Zmodem** є продовженням протоколів Xmodem та Ymodem. У ньому реалізовано таке: віконний механізм захисту від спотворення кадрів (див. 8.3); динамічна адаптація до якості каналу зв'язку шляхом зміни розміру блоку та швидкості передавання; захист інформації керування та доступу до передавання від імітації сигналів керування. Достовірність передавання

підвищується завдяки 32-розрядній контрольній комбінації. Якщо передавання файлу було припинене, то воно відновлюється з місця переривання. Протокол Zmodem використовують у каналах з високою імовірністю помилки та у високоякісних каналах як самостійно, так і з протоколами канального рівня X.25, V.42, MNP, Fastlink.

• **Kermit** – застосовують для передавання файлів між ЕОМ різних типів, у тому числі між великими та міні-ЕОМ. Він оптимізований для роботи в умовах великих завад та затримок сигналу. Протокол Super-Kermit використовує змінне вікно передавання від 1 до 32 пакетів.

8.3. Протокол HDLC, Держстандарт 26113-83

Держстандарт 26113-83 відповідає міжнародним стандартам 4335, 6256, 3309 ISO. Він описує роботу двопунктової ланки передавання даних (див. рис. 8.1).

Повний цикл функціонування двопунктової ланки передавання даних складається з таких фаз: Логічне роз'єднання, Ініціалізація, Налагодження сполучення, Передавання інформації, Завершення сполучення, Логічне роз'єднання (рис. 8.5).

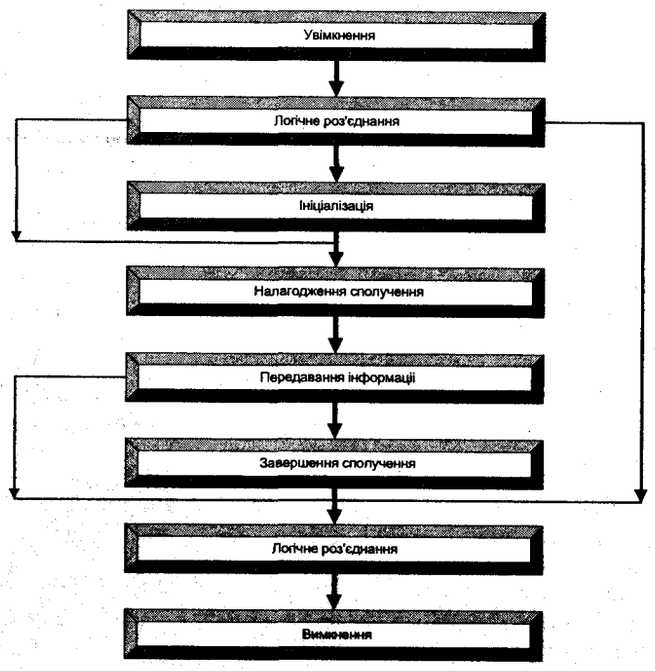


Рис. 8.5. Послідовність фаз переходу.

Логічне роз'єднання є першою і водночас останньою фазою процедур керування ланкою передавання даних, вона автоматично розпочинається після вмикання та перед вимиканням станції. Фаза *Ініціалізація* призначена для обміну інформацією про параметри програми, потрібні в інших фазах, вона є необов'язковою. Фаза *Налагодження сполучення* має на меті налагодити логічне сполучення. Фаза *Передавання інформації* – основна. У ній відбувається обмін інформацією. Після її закінчення станція переходить у фазу *Завершення сполучення*. Якщо характеристики каналу різко погіршаться, тоді можливий перехід до фази *Логічне роз'єднання* або *Налагодження сполучення*. Фаза *Завершення сполучення* є перехідною між фазами *Передавання інформації* і *Логічне роз'єднання*.

Для передавання інформації використовують три типи кадрів: інформаційний (*I*-кадр), службовий нумерований (*S*-кадр), службовий ненумерований (*U*-кадр). *I*-кадр має службову та інформаційну частини, *U*- та *S*-кадри – тільки службову. Структура службової частини кадру показана на рис. 8.6. Службова частина займає 1 байт у нерозширеному форматі і 2 байти у розширеному.

Тип кадру	Біти							
	8	7	6	5	4	3	2	1
I	N_2			P/F	N_1			0
S	N_2			P/F	s	s	0	1
U	u	u	u	P/F	u	u	1	1

Рис. 8.6. Структура кадрів протоколу HDLC.
N_1 – порядковий номер кадру, що передається; N_2 – порядковий номер кадру, який очікують.

Усі *I*-кадри з метою реалізації підтвердження нумерують. Оскільки на номер кадру в нерозширеному форматі відводиться тільки 3 біти, нумерація іде за модулем 8: 1, 2,..., 7, 0, 1,..., 7, 0,... Нумерують тільки *I*-кадри; *s*, *u* – це біти, що ідентифікують функцію *S*- або *U*-кадру; *P*/*F* – спеціальний біт з такими правилами встановлення:

1) у відповідь на правильно прийнятий *I*-кадр з бітом *P*=1 станція повинна передати у відповідь *I*- або *S*-кадр з бітом *F*=1;

2) якщо прийнято *I*- або *S*-кадр з бітом *P*=1, який спричинив некоректну ситуацію, або *U*-кадр з *P*=1, станція повинна відповісти *U*-кадром з бітом *F*=1.

Команди та відповіді протоколу

Усі кадри функціонально можна розділити на команди та відповіді. Команди наказують що зробити. Відповіді надсилаються після одержання команди. Деякі кадри можуть бути тільки командами, інші – тільки відповідями, ще інші – командами та відповідями одночасно.

Основні команди та відповіді протоколу наведені в табл. 8.1.

Таблиця 8.1. Команди та відповіді протоколу HDLC

Тип кадру	Позначення	Команда/ відповідь	Функціональне призначення кадру
I	I (Information transfer)	К, В	Переносить інформацію, підтверджує приймання
S	RR (Receive Ready)	К, В	Повідомляє про готовність до приймання
	RNR (Receive Not Ready)	К, В	Повідомляє про неготовність до приймання
	REI (Reject Information)	К, В	Повідомляє про неприймання кадрів
U	SABM (Set Asynchronous Balanced Mode)	К	Вимагає налаштувати зв'язок у нерозширеному форматі
	SABME(Set Asynchronous Balanced Mode Enlarged)	К	Вимагає налаштувати зв'язок у розширеному форматі
	FRMR (Frame Reject)	В	Повідомляє про приймання некоректного кадру
	DISC (Disconnect)	К	Вимагає припинити сполучення
	UA (Unnumbered Acknowledgment)	В	Підтверджує згоду на виконання команди
	DM (Disconnect Mode)	В	Повідомляє про незгоду виконати команду або про наявність режиму роз'єднання
	SIM (Set Initialization Mode)	К	Вимагає провести ініціалізацію передаванням параметрів на віддалену станцію
	RIM (Reset Initialization Mode)	В	Вимагає провести ініціалізацію прийманням параметрів з віддаленої станції
	UI (Unnumbered Information)	К, В	Ненумерований інформаційний кадр

Розглянемо роботу протоколу HDLC у різних фазах.

Фаза *Логічне роз'єднання*

Перехід у фазу *Логічне роз'єднання* може відбутися за однієї з таких умов:
- увімкнення станції;
- закінчення виконання процедур фази *Завершення сполучення*;
- передавання кадру DM.

У фазі *Логічне роз'єднання* станція аналізує всі прийняті з каналу кадри.

- Якщо в прийнятому кадрі виявлена команда DISC, то станція повинна відповісти кадром DM. Значення бітів *P* та *F* у цих кадрах збігаються.
- Якщо в прийнятому кадрі виявлена команда SABM (SABME), то станція переходить у фазу *Налагодження сполучення*.
- Якщо в прийнятому кадрі виявлені команди SIM або RIM, то станція переходить у фазу *Ініціалізація*.
- Якщо прийнято інший кадр, у якому P=1, то станція повинна відповісти кадром DM F=1.
- Інші прийняті кадри не беруться до уваги.

Вийти з фази *Логічне роз'єднання* можна у таких випадках:
- приймання з каналу кадру SABM або SABME (перехід у фазу *Налагодження сполучення*);
- приймання з каналу кадру SIM або RIM (перехід у фазу *Ініціалізація*);
- одержання вимоги від протоколу верхнього рівня про налагодження сполучення (перехід у фазу *Налагодження сполучення*);
- одержання вимоги від протоколу верхнього рівня про введення параметрів на віддалену станцію або виведення з неї (перехід у фазу *Ініціалізація*);
- вимкнення станції.

Фаза *Ініціалізація*

Для переходу у фазу *Ініціалізація* потрібно таке:
- приймання з каналу кадру з командою SIM;
- приймання з каналу кадру з відповіддю RIM;
- одержання вимоги від протоколу верхнього рівня про введення параметрів на віддалену станцію або виведення з неї.

Кожна станція інформує про намір перейти у фазу *Ініціалізація* передаванням кадру з командою SIM (якщо треба ввести параметри на віддалену станцію), або відповіддю RIM (якщо треба скоректувати дані та прийняти для цього інформацію з віддаленої станції). Після передавання кадру з командою SIM станція починає відлік тайм-аутів T_1 та T_2. Віддалена станція, яка одержала SIM, відповідає кадром UA, занулює лічильники V_1 і V_2 та таймери. Якщо станція, яка правильно прийняла SIM, визначає, що не може перейти у фазу *Ініціалізація*, то вона відповідає кадром DM та переходить у фазу *Логічне роз'єднання*.

Якщо команди SIM, відповіді UA, DM прийняті неправильно, то їх не враховують. Тоді на станції, яка передала SIM, закінчується тайм-аут T_1, і вона повторює надсилання SIM. Так буде тривати доти, доки не закінчиться $T_2 >> T_1$. Потім станція повідомляє верхньому рівню про неможливість провести ініціалізацію та переходить у фазу *Логічне роз'єднання*. Надалі подібну процедуру називатимемо таймерною.

Обмін інформацією у фазі *Ініціалізація* відбувається з використанням кадрів UI та I.

Вийти з фази *Ініціалізація* можна у таких випадках:
- приймання команди DISC (перехід у фазу *Завершення сполучення*);
- приймання команди SABM (перехід у фазу *Налагодження сполучення*);

• приймання команди DM (перехід у фазу *Логічне роз'єднання*);
• закінчення T_2 (перехід у фазу *Логічне роз'єднання*);
• одержання вимоги від протоколу верхнього рівня про перехід у фазу *Налагодження сполучення* (перехід у фазу *Налагодження сполучення*);

Фаза *Налагодження сполучення*

У фазу *Налагодження сполучення* можна перейти у випадку:
• приймання кадру з командою SABM;
• одержання від протоколу верхнього рівня сигналу про налагодження сполучення.

Кожна станція, яка отримала від верхнього рівня сигнал про налагодження сполучення, надсилає іншій станції кадр з командою SABM і починає відлік тайм-аутів T_1 та T_2. Станція, яка правильно прийняла SABM, повинна відповісти UA, занулити лічильники V_1 та V_2 і таймери. Якщо відповіді на команду SABM не одержано, розпочинається таймерна процедура. Після закінчення T_1 станція знову повторює команду SABM, а після закінчення T_2 повідомляє про це протокол верхнього рівня і переходить у фазу *Логічне роз'єднання*.

Якщо станція, яка одержала кадр з командою SABM, не може налагодити сполучення, то вона відповідає DISC. Станція, що одержала DISC, переходить у фазу *Завершення сполучення*.

Вийти з фази *Налагодження сполучення* можна за таких умов:
• приймання кадру UA у відповідь на передану команду SABM (перехід у фазу *Передавання інформації*);
• передавання в канал кадру UA у відповідь на прийняту команду SABM (перехід у фазу *Передавання інформації*);
• закінчення тайм-ауту T_2 (перехід у фазу *Логічне роз'єднання*);
• приймання кадру DISC (перехід у фазу *Завершення сполучення*).

Фаза *Передавання інформації*

Перехід у фазу *Передавання інформації* може відбутися за умов:
• приймання з каналу кадру UA у відповідь на надісланий SABM;
• передавання відповіді UA на прийнятий кадр SABM.

З метою полегшити розуміння та опис процедур фази *Передавання інформації* введено шість станів: *Передавання*, *Зайнято*, *Зупинка*, *Блокування*, *Часова витримка*, *Неприймання кадру*. Деякі стани можуть перетинатися у часі. Проте кожна станція не може бути більш ніж у двох станах одночасно. Якщо станція перебуває у двох станах, то вона повинна виконувати дії, передбачені кожним станом, та не виконувати дій, заборонених хоча б одним зі станів.

Стан *Передавання*

Стан *Передавання* буває у випадку, коли нема завад та наявне правильне передавання у каналі. Інформація, одержана від протоколу верхнього рівня, розміщується в інформаційному полі *I*-кадру та передається. Така ж процедура відбувається в зворотному напрямі. Для забезпечення правильної послідовності кадрів кожен *I*-кадр нумерується за модулем деякого числа *M*. За правильністю нумерації стежить лічильник V_1, який визначає номер кадру, що передається. Значення V_1 розміщується в полі N_1 кадру. Кожного разу після передавання кадру значення V_1 збільшується на 1.

Під час приймання станція стежить за номерами одержуваних кадрів та передає їх верхньому рівню відповідно до послідовності номерів. Номер кадру, який треба прийняти, зберігається у лічильнику V_2. Якщо прийнято очікуваний номер кадру, то V_2 збільшується на 1, якщо ж прийнято кадр, номер якого більший або менший від V_2, то його станція відкидає. Значення лічильника V_2 записується у полі N_2 *I*-кадру. Якщо станція не має інформації для передавання, то вона надсилає кадр RR з полем N_2. Підтвердженими вважаються всі кадри, номер яких менший або дорівнює N_2–1. Кількість переданих, але не підтверджених кадрів не може перевищувати *M*. Максимальна кількість $K \le M-1$ називається вікном та залежить від внутрішніх параметрів станції. Якщо станція зауважила, що кількість переданих, однак не підтверджених кадрів дорівнює *K*, то вона не має права передавати нові кадри, а тільки повторює попередні.

Стан *Зайнято*

Стан *Зайнято* буває тоді, коли станція внаслідок внутрішніх причин не може прийняти *I*-кадр. У цьому випадку вона надсилає іншій станції кадр RNR, який спричинює там стан *Зупинка*. Перебуваючи у стані *Зайнято*, станція повинна приймати *S*-кадри та службову частину *I*-кадрів, а також передати кадр RNR з бітом F=1, якщо одержала *S*- або *I*-кадр з бітом P=1. Станція не може збільшувати значення лічильника V_2. Якщо станція може прийняти *I*-кадр, то вона надсилає іншій станції кадр RR і переходить у стан *Передавання*.

Стан *Зупинка*

Стан *Зупинка* настає в результаті правильного приймання кадру RNR. У цьому стані станція не може передавати *I*-кадри, крім найстаршого з непідтверджених *I*-кадрів з бітом P=1. Це робиться з метою вивести іншу станцію зі стану *Зайнято*. Якщо ж інша станція не готова до приймання, то вона надсилає у відповідь кадр RNR (F=1).

Стан *Блокування*

Стан *Блокування* трапляється тоді, коли внаслідок спотворення деяка кількість *I*-кадрів втрачена. У цьому випадку порушується порядок передавання кадрів і виникає потреба повторити їх.

Визначено чотири режими повторення кадрів: *основний* (В), *квазіадресний* (К), *селективний* (С), *адресний* (А). Реалізація всіх режимів не є обов'язковою. Як звичайно, завжди є основний режим. Наявність інших режимів залежить від конкретної реалізації протоколу.

Режим В ґрунтується на використанні правил передавання біта *P*/*F*. Надсилаючи кадр з бітом P=1, станція передавання розпочинає відлік тайм-аутів T_1 та T_2. Інша станція, що одержала кадр з бітом P=1, повинна відповісти *S*- або *I*-кадром з бітом F=1. Станція передавання, одержавши відповідь, занулює таймери T_1 та T_2 й аналізує поле N_2 в прийнятому кадрі. Якщо поле N_2 підтверджує приймання всіх кадрів аж до V_1, то повторення кадрів не потрібне. В іншому

випадку лічильник V_1=N_2, і відбувається повторення всіх кадрів, починаючи з N_2. Якщо тайм-аут T_1 закінчився, а відповіді нема, то повторюється передавання кадру з P=1 і вмикається таймерна процедура. Кадр з бітом P=1 передається періодично, однак тривалість періоду не може перевищувати розміру вікна.

Режим К подібний до режиму В, однак станція приймання, ще не прийнявши кадр з бітом P=1, може надіслати кадр REI, у якому поле N_2 дорівнює V_2. Станція передавання скоригує значення лічильника V_1.

Режим С дає змогу повторити тільки один деякий *I*-кадр. Станція, яка перебуває у стані *Блокування*, надсилає кадр SREI, у якому N_2 дорівнює номеру потрібного кадру. Станція передавання, прийнявши кадр SREI, надсилає цей кадр. Станція приймання повинна зберігати всі правильно прийняті кадри після кадру, на який надіслано запит.

Режим А, як і режим С, дає змогу у відповіді на запит повторити тільки один *I*-кадр. Станція, яка перебуває у стані *Блокування*, надсилає пакет кадрів AREI, у яких N_2 набуває значення номерів неприйнятих кадрів. Упродовж правильного приймання значення лічильника V_2 коригується та надсилаються нові кадри AREI. У випадку надсилання AREI запускається тайм-аут T_3. До його закінчення надсилати кадри з однаковими N_2 забороняється. Правильно прийнявши AREI, станція надсилає бажаний кадр і продовжує передавати дані. Якщо T_3 закінчився, а відповіді нема, то станція повторює AREI.

Стан *Часова витримка*

Стан *Часова витримка* пов'язаний з передаванням поодиноких кадрів або з тривалим впливом завад у каналі. Якщо на переданий кадр довго нема ніякої відповіді, то неможливо перейти в стан *Блокування* і повторити кадри. Тому після кожного надсилання кадру (I, RR, RNR, REI, SREI) станція стежить за сигналом зворотного зв'язку. Будь-коли, якщо на станції є передані, але не підтверджені кадри, вона починає відстежувати тайм-аут T_1. Якщо тайм-аут закінчився, а підтвердження не надійшло, то станція переходить у стан *Часова витримка* (якщо вона не перебуває у стані *Зупинка*). У цьому стані вона не має права передавати *I*-кадри, крім найстаршого *I*-кадру з бітом P=1. Після передавання цього кадру станція вмикає таймерну процедуру, а після закінчення T_2 повідомляє протокол верхнього рівня про неможливість передавання інформації та переходить у фазу *Завершення сполучення*.

Стан *Неприймання кадру*

Стан *Неприймання кадру* настає тоді, коли код, що коригує помилки, не в змозі виявити помилку, тобто на станцію надходить нечинна команда або кадр незрозумілого формату, або не дійсне N_2 тощо. У цьому випадку будь-який інший стан неможливий. На іншу станцію надсилається кадр FRMR або RESET (якщо N_2 недійсне). У стані *Неприймання кадру* станція не опрацьовує жодні *I*- та *S*-кадри і не передає їх, крім кадру FRMR. Станція, яка правильно прийняла кадр FRMR, повідомляє про це протокол верхнього рівня і передає кадр SABM, переводячи обидві станції у фазу *Налагодження сполучення*.

Станція, яка передала кадр RESET, вмикає T_1. Інша станція, прийнявши RESET, занулює V_2 і відповідає кадром UA. Станція, одержавши кадр UA, занулює V_1 і переходить у стан *Передавання*. У цьому випадку всі непідтверджені кадри повинні бути повернені джерелу інформації або знищені. Якщо T_1 закінчився, а відповіді UA немає, то станція надсилає FRMR.

Передавання та приймання *UI*-кадрів може відбуватися у всіх станах фази *Передавання інформації*.

Вийти з фази *Передавання інформації* можна у таких випадках:

- приймання команди SABM (перехід у фазу *Налагодження сполучення*);
- приймання команди DISC (перехід у фазу *Завершення сполучення*);
- приймання команди SIM (перехід у фазу *Ініціалізація*);
- одержання від протоколу верхнього рівня сигналу про завершення сполучення (перехід у фазу *Завершення сполучення*);
- приймання відповіді DM (перехід у фазу *Логічне роз'єднання*).

Фаза *Завершення сполучення*

У фазу *Завершення сполучення* можна перейти за умов:

- одержання від протоколу верхнього рівня сигналу про завершення сполучення;
- приймання команди DISC.

Будь-яка станція, яка одержала від протоколу верхнього рівня сигнал про завершення сполучення, передає в канал кадр DISC та розпочинає відлік тайм-аутів T_1 і T_2. Інша станція, одержавши DISC, переходить у фазу *Завершення сполучення*, повідомляє про це протокол вищого рівня та відповідає UA. Після цього вона переходить у фазу *Логічне роз'єднання*. Станція, яка у відповідь на DISC одержала UA- або DM-кадри, переходить у фазу *Логічне роз'єднання*. Якщо відповіді на DISC нема, то вмикається таймерна процедура. Станція, перебуваючи у стані *Завершення сполучення*, інші команди ігнорує.

Вийти з фази *Завершення сполучення* можна за таких умов:

- приймання кадрів UA або DM у відповідь на надісланий кадр DISC (перехід у фазу *Логічне роз'єднання*);
- передавання кадру UA у відповідь на прийнятий кадр DISC (перехід у фазу *Логічне роз'єднання*);
- закінчення тайм-ауту T_2 (перехід у фазу *Логічне роз'єднання*).

Бібліографія та джерела

1. *Вильховченко С.* Модем 96. М.: ABF, 1996.
2. *Девис Д., Барбер Д., Прайс У., Соломонидес С.* Вычислительные сети и сетевые протоколы. М.: Мир, 1982.
3. *Мартин Д.* Вычислительные сети и распределенная обработка данных. Программное обеспечение, методы и архитектура. В 2 т. М.: Финансы и статистика, 1985.
4. *Мартин Дж.* Системный анализ передачи данных. В 2 т. М.: Мир, 1995.
5. *Халсалл Ф.* Передача данных, сети компьютеров и взаимосвязь открытых систем. М.: Радио и связь, 1995.

ПРОТОКОЛИ МЕРЕЖЕВОГО ТА ТРАНСПОРТНОГО РІВНІВ

Головні функції протоколів мережевого та транспортного рівнів. Мережевий рівень. Даграмна стратегія та стратегія віртуальних каналів. Їхнє порівняння. Віртуально-даграмний протокол X25/3. Структура пакета для віртуального виклику та даграми. Комплекс протоколів XSIS. Міжмережевий даграмний протокол фірми XEROX. Транспортний рівень. Його головні функції та класи сервісу. Протоколи XSIS: луна, обмін пакетами, нумеровані пакети.

Канальний рівень забезпечує зв'язок між двома сусідніми станціями, як звичайно, в одній мережі. Якщо ж треба сполучити кілька станцій з проміжними вузлами опрацювання або локальну мережу з іншою мережею (локальною або глобальною), користуються *мережевим рівнем*. Одна з головних функцій мережевого рівня – побудова маршруту руху пакета в мережі з багатьма вузлами (маршрутизація). У простих локальних мережах цей рівень використати не можна. *Транспортний рівень* пов'язує окремі процеси, які виконують певні функції (рис. 9.1).

9.1. Мережевий рівень

Мережевий рівень призначений для організації зв'язку станцій, при'єднаних до різних логічних каналів та, можливо, роз'єднаних іншими логічними каналами. Функції мережевого рівня, головним чином, полягають у вибиранні послідовності каналів між станціями під час передавання протокольного блоку даних на рівні мережі, тобто пакета. Історично перші протоколи рівня мережі були розроблені для ГМ. Це пояснюється тим, що глобальні мережі є багатовузловими і досягнення ефективної маршрутизації – одна з головних проблем у їхній роботі. Водночас з'явилися також поняття стратегій передавання: *даграмної та віртуальних каналів.*

Даграмною називається така транспортна мережа, в якій передаються окремі, не пов'язані між собою пакети – даграми. Характер роботи мережі подібний до роботи пошти: окремі листи незалежні, їх можна загубити.

У мережі **віртуальніх каналів** перед початком передавання між парою процесів налагоджується постійне сполучення – віртуальний канал, що функціонує протягом усього сеансу зв'язку. Робота мережі віртуальних каналів аналогічна до роботи телефонної мережі. Перед початком сполучення налагоджується канал зв'язку, послідовність інформації, що передається, зберігається.

Даграмна мережа надсилає пакети значно швидше, ніж мережа віртуальних каналів, однак гарантії, що пакет дійде до адресата, немає (порядок надходження пакетів випадковий; можлива втрата пакетів та переповнення буферів).

У мережі віртуальних каналів зв'язок відбувається повільніше, проте є гарантія, що пакет дійде до адресата (порядок надходження пакетів зберігається, якщо вузол переповнений, надходження пакетів від джерела припиняється).

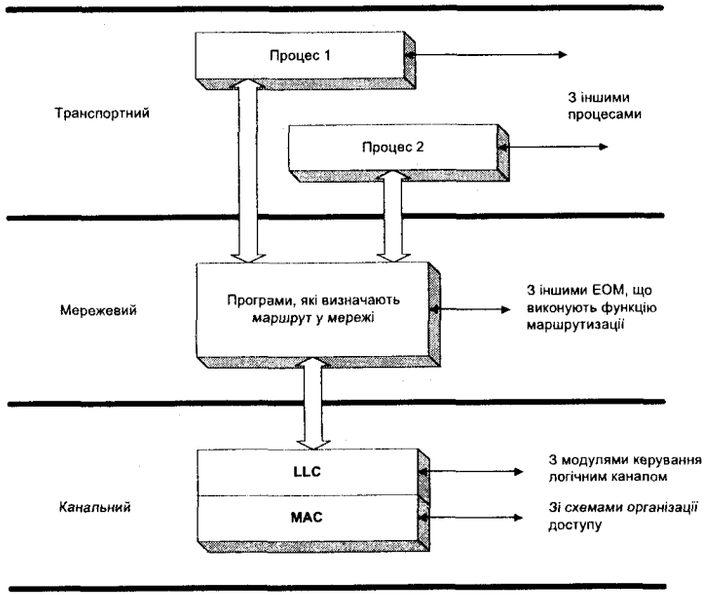


Рис. 9.1. Структура зв'язків канального, мережевого та транспортного рівнів.

Протокол X.25/3

Одним з найвідоміших протоколів мережевого рівня є протокол X.25/3, розроблений ITU в 1976 р. і затверджений стандартом 8208 ISO. Стандарт 8881 ISO визначає використання протоколу X.25 у ЛМ, однак у цьому випадку потрібне узгодження з підрівнем керування логічним каналом LLC.

Протокол X.25 описує віртуально-даграмну мережу, тобто мережу віртуальних каналів, у якій за певних умов можна передавати даграми. Відповідно до протоколу X.25/3 у транспортній мережі між абонентами налагоджуються тимчасові (на один сеанс зв'язку) та постійні віртуальні транспортні канали. Тимчасовий канал називається віртуальним викликом, постійний – віртуальним ланцюжком. Кожному віртуальному виклику або ланцюжку присвоюється номер групи віртуальних каналів (0–15) та номер окремого віртуального каналу (0–255). Номери віртуальних викликів змінюються циклічно у міру їх створення та знищення. Номери віртуальних ланцюжків зберігаються довше.

Структура мережевої адреси описана в рекомендації X.121 ITU (рис. 9.2).

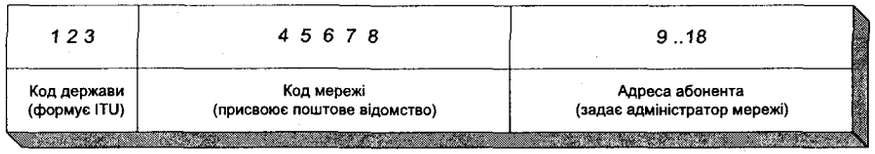


Рис. 9.2. Структура мережевої адреси.

Після налагодження віртуального каналу пакети передаються почергово. Механізм підтвердження та виправлення помилок подібний до механізму протоколу HDLC. Структура пакета віртуального виклику або ланцюжка показано на рис. 9.3.

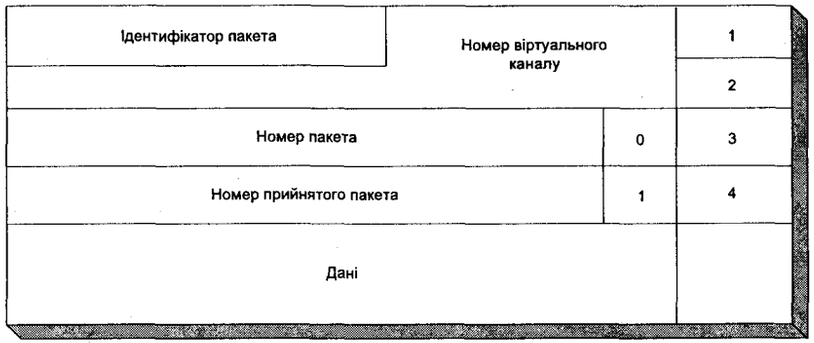


Рис. 9.3. Структура пакета віртуального виклику.

У випадку використання протоколу для данограмного передавання один або декілька віртуальних каналів резервуються для данограм, послідовність передавання, а також саме передавання не гарантовані. Структура данограмного пакета зображений на рис. 9.4.

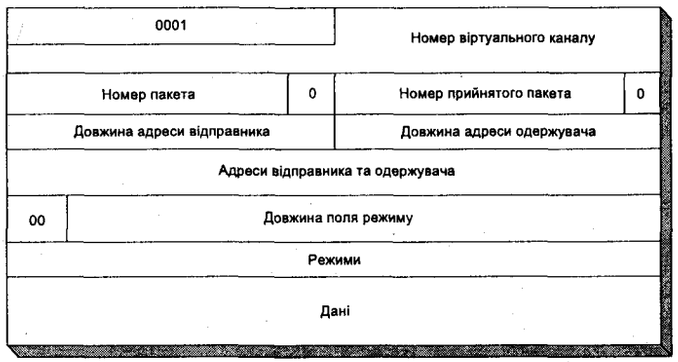


Рис. 9.4. Структура данограмного пакета.

Міжмережевий данограмний протокол фірми XEROX

Перший набір протоколів мережевого та канального рівнів, спеціально призначених для використання в ЛМ, розроблений у 1981 р., коли фірма XEROX почала публікувати серію протоколів *XSIS (Xerox System Integration Standards)*. Детальніше розглянемо міжмережевий данограмний протокол фірми XEROX.

Такий протокол призначений для обслуговування систем, які об'єднують одну або кілька мереж Ethernet, сполучених орендованими каналами зв'язку ГМ, що побудовані за стандартом X.25. Можливе приєднання інших локальних та глобальних мереж. Максимальна кількість проміжних каналів між двома віддаленими ЛМ не може перевищувати 14. Дані та інформація керування передаються у вигляді міжмережевих данограм. Структура пакета такої данограми показано на рис. 9.5.

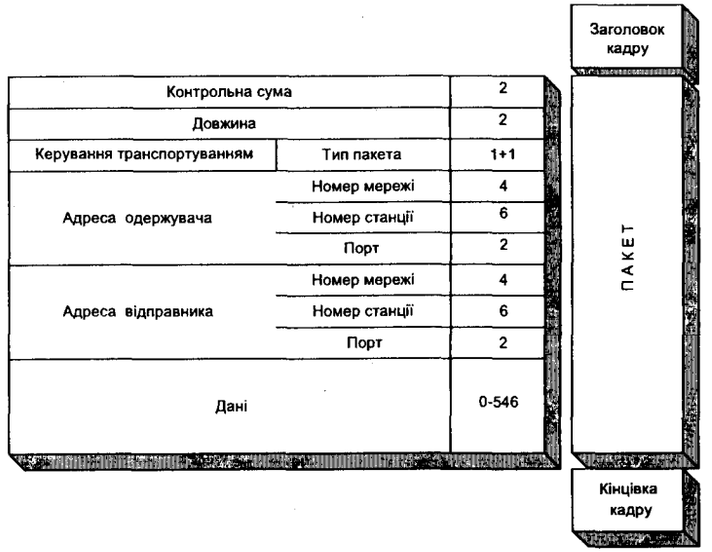


Рис. 9.5. Структура пакета міжмережевого данограмного протоколу.

Як бачимо з рис. 9.5, цей пакет може стати елементом кадру та передаватися на канальному рівні. Адреси (одержувача та відправника) мають ієрархічну структуру:

номер мережі – номер станції – порт.

Номер мережі може задавати мережу типу Ethernet або будь-яку іншу, в яку надсилають пакет. Номер станції – це внутрішня адреса станції у мережі. Оскільки структура адреси ієрархічна, то номери станцій у різних мережах можуть дублюватися. Можна також надіслати пакет усім станціям мережі одночасно: для цього є спеціальний номер. Порт – це дані транспортного

рівня, точка контакту з ним. Номер порту визначає певну програму або модуль опрацювання, якому призначено пакет; він займає 16 біт. Номери від 1 до 3000 зарезервовані. Зокрема, номер 1 відповідає *Маршрутній інформації*, 2 – *Луні*, 3 – *Помилкам маршруту*, 5 – *Протоколу кур'єра.*

Поле *Тип пакета* призначене для вибору відповідного транспортного протоколу. Для цього серед інших визначені такі коди:

1 – Маршрутна інформація;
2 – Луна;
3 – Помилка;
4 – Обмін пакетами;
5 – Нумеровані пакети.

Байт керування транспортуванням у старших чотирьох бітах має лічильник кількості передавань пакета з однієї мережі в іншу. Пакет, що надходить у 16-й за порядком модуль маршрутизації, знищується. Це дає змогу запобігти зациклюванню пакетів у великих мережах.

9.2. Транспортний рівень

Транспортний рівень керує взаємодією процесів, а не станцій, мереж чи каналів (див. рис. 9.1). Відповідно до міжнародних стандартів протокол транспортного рівня повинен задовольняти такі вимоги:

1) забезпечувати *наскрізне* передавання. Характеристики транспортного сервісу не залежать від типу комунікаційної мережі або мереж;

2) користувач транспортного рівня має змогу *вибрати якість сервісу*, що передбачає вибір перепускної здатності, транзитної затримки, коефіцієнта невиявлених помилок тощо;

3) транспортний сервіс є *прозорим*, тобто не залежить від форматів та кодів інформації, що передається;

4) адресація на транспортному рівні не залежить від адресації на інших рівнях. Транспортні об'єкти мають унікальні адреси.

Транспортний протокол, як і протоколи інших рівнів, специфікує команди та правила їх використання. Головні функції транспортного рівня такі:

- налагодження сполучення;
- узгодження партнерами якості сервісу;
- передавання звичайних даних;
- передавання термінових даних;
- керування потоками блоків даних;
- аварійне розірвання сполучення;
- нормальне завершення сполучення.

Під час вибирання якості сервісу узгоджують застосування таких функцій:

- забезпечення взаємодії кількох транспортних сполучень з одним мережевим (мультиплексування) або, навпаки, одного транспортного сполучення з кількома мережевими;

- вибір оптимального розміру транспортних блоків;
- використання функції виявлення та виправлення помилок;
- узгодження допустимої частоти помилок (втрата, дублювання або спотворення даних);
- здатність транспортного рівня до поновлення після збоїв;
- регулювання перепускної здатності сполучення.

Європейська асоціація виробників комп'ютерів у 1981 р. затвердила транспортний протокол ECMA-72, який визначає чотири класи транспортного сервісу. Пізніше ISO та ITU додали ще один клас.

- Клас 0 призначений для використання в найпростіших системах. Він налагоджує транспортне сполучення, керує ним, однак клас 0 не перевіряє правильність переданої інформації, не виправляє помилок та не дає змоги застосувати мультиплексування.
- Клас 1 виконує всі функції класу 0, а також гарантує контроль інформації з виявленням та виправленням помилок.
- Клас 2 виконує всі функції класу 0 і, крім того, допускає мультиплексування.
- Клас 3 є комбінацією класів 1 та 2. Сумісний з класами 0, 1, 2.
- Клас 4 виконує найповніший набір функцій: мультиплексування та найповніше виправлення помилок; перевіряє та формує прийняту послідовність блоків даних; забезпечує роботу на мережевому рівні не тільки віртуальних каналів (класи 0–3), але й даграм.

Дуже часто один мережевий рівень підтримує кілька різних транспортних протоколів, які забезпечують різні рівні обслуговування. Наприклад, практично використовують такі різновиди транспортних потоків:

- передавання суцільного потоку даних з малою затримкою відповіді; можна використовувати в цифровій телефонії та для передавання графічної інформації;
- передавання даграм з квитанціями; використовують для організації доступу до деяких видів файлів;
- передавання нумерованих пакетів; застосовують для транспортування файлів, електронної пошти.

Набір протоколів XSIS має кілька транспортних протоколів, зокрема *Луна, Обмін пакетами, Нумеровані пакети, Помилка, Маршрутна інформація.*

Простий **протокол *Луна*** призначений для перевіряння цілісності мережі та готовності станцій до взаємодії. Цьому протоколу відповідає тип пакета 2 та порт 2. Структура пакета протоколу *Луна* показано на рис. 9.6.

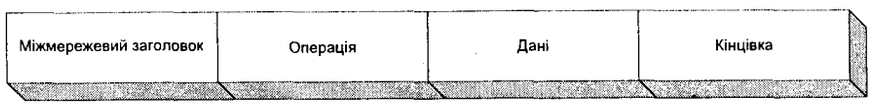


Рис. 9.6. Структура пакета *Луна*.

Станція, яка прийняла пакет протоколу *Луна*, замінює в полі *операція* код запиту (1) на код відповіді (2) та надсилає пакет станції-відправнику. Якщо пакет *Луна* спотворений, то повідомлення про це передають засоби протоколу *Помилка*.

Протокол *Обмін пакетами* використовують для таких операцій, як запит про стан станції або час доби. Він не забезпечує цілісності даних та надійності передавання. Пакети цього протоколу мають тип 4. Структура пакета зображено на рис. 9.7.

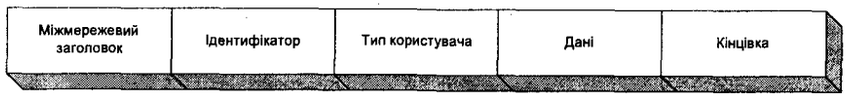


Рис. 9.7. Структура пакета протоколу *Обмін пакетами.*

Поле *Ідентифікатор* ідентифікує номер поточного обміну, а поле *Тип користувача* відповідає порту призначення. Відправник, який надіслав запит, чекає на відповідь. Якщо відповіді немає, то запит повторюється.

Протокол *Нумеровані пакети* є протоколом віртуального виклику, який підтримує взаємодію процесів. Він дає змогу надсилати повідомлення, що складаються з багатьох пакетів, гарантує цілісність і правильну їх послідовність, а також організовує повторне передавання спотворених пакетів. Дані пересилаються як міжмережеві данограми з типом пакета 5. Структура пакета показано на рис. 9.8.

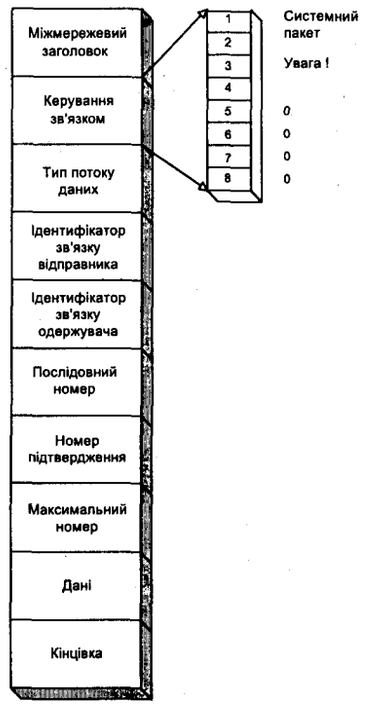


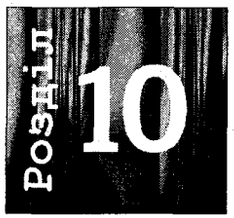
Рис. 9.8. Структура пакета протоколу *Нумеровані пакети.*

Поле *Ідентифікатор зв'язку* призначене для адресування. Спочатку, щоб налагодити віртуальний виклик, станція відправляє пакет з ідентифікатором відправника (ідентифікатор одержувача може бути невідомий) на адресу потрібного порту. Станція-одержувач записує свій ідентифікатор у перший пакет відповіді. Далі відбувається передавання пакетів інформації. Правильність приймання підтверджує інформація у полі *Номер підтвердження*. Квитанції можуть відсилатися як на окремий пакет, так і на групу. Виняток становлять пакети з бітом *Відіслати підтвердження*. Квитанції для таких пакетів відсилаються негайно. Поле *Максимальний номер* призначене для керування потоком. Станція-одержувач дає станції-передавачу максимальний номер, яким вона може скористатися для нумерації пакетів. Значення цього поля змінюється після кожного надсилання квитанції. У полі *Послідовний номер* записують номер пакета, який надсилають. Поле *Тип потоку даних* призначене для протоколу сеансового рівня. Біт 4 у полі керування зв'язком – *Кінець повідомлення* також призначений для протоколу верхнього рівня. За ним можна зафіксувати кінець повідомлення, що складається з багатьох пакетів (логічний запис, фізичний блок на диску тощо). Для закінчення віртуального виклику в полі *Тип потоку даних* записують код *254* (кінець), на що станція-одержувач відповідає значенням у цьому полі *255*.

Пакет може не мати даних, а бути системним, його використовують для підтвердження і керування потоком. Пакет, у якому є біт *Увага!*, у випадку одержання відразу передається протоколу верхнього рівня.

Бібліографія та джерела

1. *Мартин Д.* Вычислительные сети и распределенная обработка данных. Программное обеспечение, методы и архитектура: В 2 т. М.: Финансы и статистика, 1985.
2. *Флинт Д.* Локальные сети ЭВМ: архитектура, принципы построения, реализация /Пер. с англ. М.: Финансы и статистика, 1986.
3. *Халсалл Ф.* Передача данных, сети компьютеров и взаимосвязь открытых систем. М.: Радио и связь, 1995.



МЕТОДИ МАРШРУТИЗАЦІЇ

Проблема маршрутизації. Класифікація методів маршрутизації. Прості та складні методи. Випадкова, лавинна, фіксована, адаптивна маршрутизації. Маршрутизація 'за досвідом'. Метод якнайшвидшого передавання. Локально-адаптивна маршрутизація. Розподілена маршрутизація. Централізована та гібридна маршрутизації.

У цьому розділі коротко описано методи, розроблені для вирішення проблеми маршрутизації інформації у глобальних мережах. Не всі з них використовують на практиці, більшість є надбанням теорії. Знання методів маршрутизації дає змогу оцінити загальні способи вирішення проблеми маршрутизації в мережах та порівняти реальні алгоритми маршрутизації. (Порівняйте з алгоритмами маршрутизації мереж протокольних стеків SPX/IPX (Novell Netware) та TCP/IP (Unix), розділ 13).

Проблема маршрутизації, як уже зазначалося, полягає у виробленні маршруту, по якому рухається пакет у багатовузловій мережі. Цей маршрут повинен задовольняти певні вимоги. Найчастіше потрібно мінімізувати час проходження пакета мережею. Маршрутизацію переважно забезпечують розміщенням у вузлах мережі маршрутної інформації (маршрутних таблиць) та програм, які реалізують алгоритм маршрутизації (залежно від адреси призначення та маршрутної інформації обирають наступний вузол передавання пакета).

Наведемо класифікацію методів маршрутизації (рис. 10.1).

Усі методи маршрутизації умовно поділяють на *прості* та *складні*. Прості методи маршрутизації не потребують у вузлах мережі маршрутних таблиць та складного програмного забезпечення.

До простих методів маршрутизації належать *випадкова* та *лавинна (циркулярна)* маршрутизації.

Випадкова маршрутизація полягає в тому, що вузол, який одержав транзитний (не призначений йому) кадр, пересилає його в один із своїх вихідних каналів. Канал вибирається випадково та рівноймовірно. Щоб запобігти безмежному блуканню пакета у мережі, у нього вмонтовують лічильник кількості пройдених вузлів. Якщо значення лічильника вузлів перевищило певне число, пакет знищується. Такий метод маршрутизації не оптимальний, не гарантує передавання пакета адресату, створює значний додатковий трафік у мережі. На практиці його не використовують.

У випадку **лавинної** маршрутизації кожен вузол передає транзитний пакет, що надійшов до нього, у всі вихідні канали. Як і у випадковій маршрутизації, кожен пакет має лічильник кількості пройдених вузлів. Лавинна маршрутизація генерує значний трафік у мережі, однак гарантує передавання пакета (порівняйте з циркулярним передаванням, розділ 13, яке широко використовують).

Складні методи маршрутизації поділяють на детерміновані та адаптивні. Методи **детермінованої маршрутизації** у проміжних вузлах передбачають використання таблиць маршрутизації або набори таблиць, які не змінюються залежно від стану мережі (точніше, їх змінюють вручну). Методи **адаптивної маршрутизації** гнучкіші, тобто маршрутна інформація може змінюватися залежно від завантаженості окремих ланок мережі, виходу їх з ладу тощо.

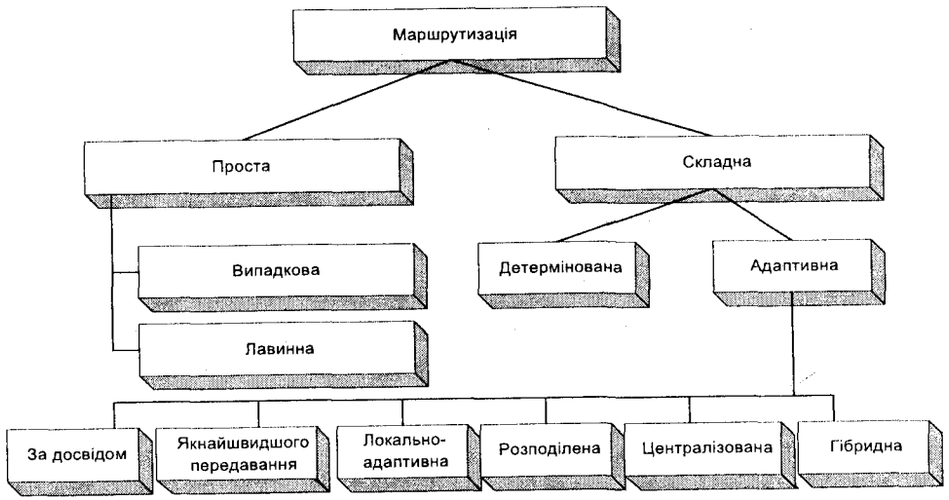


Рис. 10.1. Класифікація методів маршрутизації.

Методи детермінованої маршрутизації ефективні для малозавантажених мереж. Зі збільшенням завантаження їхня ефективність швидко зменшується. Є варіанти детермінованої маршрутизації з набором таблиць, кожна з яких враховує вихід з ладу конкретних каналів, а також таблицями, які реалізують розщеплення потоку у вузлі в певній пропорції, наприклад 60–40% (рис. 10.2).

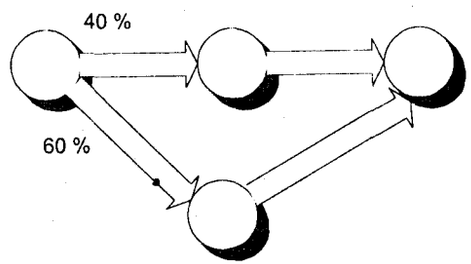


Рис. 10.2. Розщеплення інформаційного потоку.

Адаптивна маршрутизація ґрунтується на ідеї пристосування алгоритму до реального стану мережі. Під час досліджень цього методу були виявлені деякі обмеження. Наприклад,

уявимо собі деяку інстанцію регулювання у мережі, яка в кожен момент часу має повну інформацію про стан мережі і на підставі цього надає маршрутну інформацію для всіх інших вузлів (метод ідеального спостерігача). Навіть у цьому ідеальному випадку маршрутна інформація є старітиме, оскільки весь трафік буде спрямовуватись у тимчасово вільні канали, що призведе до їх перевантаження. Слабкою стороною такого підходу є неможливість передбачити стан мережі.

Нижче опишемо методи адаптивної маршрутизації.

• **Маршрутизація 'за досвідом'**. Спочатку транзитні пакети кожного вузла спрямовують у випадкові вихідні канали. Однак кожен пакет, крім адрес відправника та одержувача, має лічильник кількості пройдених каналів. Вузол аналізує цю інформацію і будує таблицю найближчих вузлів у випадку надсилання пакета до конкретного адресата. Після закінчення побудови таблиць вузол працює в режимі детермінованої маршрутизації.

• **Метод якнайшвидшого передавання**. Станції ставлять за мету якнайшвидше позбутися транзитного пакета. Для кожного вихідного каналу фіксують час, коли той передавав пакет певному адресату. Таку інформацію читають з відповідного поля кожного пакета. У цьому методі, крім інформації про час передавання, використовуть інформацію про наявність та довжину черг до вихідних каналів.

• **Локально-адаптивна маршрутизація**. Висновок про спрямування пакета в конкретний вихідний канал робиться на підставі тільки локальної інформації. Такою локально доступною інформацією є наявність та довжина черг до вихідних каналів.

• **Розподілена маршрутизація**. У кожному вузлі зберігаються маршрутні таблиці, в яких зазначено маршрути до кожного з адресатів з мінімальною затримкою передавання. Спочатку такі таблиці будують на підставі теоретичного розрахунку за відомою топологічною структурою мережі. Потім ці дані постійно оновлюють на підставі вимірювань. Для цього в мережі повинен бути трафік маршрутної інформації. Розподілену адаптивну маршрутизацію найчастіше використовують у реальних мережах. Зокрема, у мережі Internet на початку її функціонування вузли аналізували транзитний потік, визначали час передавання пакетів та будували таблиці з зазначенням часу передавання пакета до сусідніх вузлів. Вузли регулярно обмінювались такими таблицями затримок, що призводило до виникнення додаткового трафіка маршрутизації, який досягав 50% корисного трафіка. З часом в алгоритмі маршрутизації Internet було зроблено корективи. Тепер маршрутні таблиці передають тільки ті вузли, які виявили значну зміну інтенсивності трафіка або значні відхилення в стані функціональних компонент. Це дало змогу різко зменшити трафік маршрутизації та зробити роботу мережі стабільнішою.

• **Централізована маршрутизація**. У мережах з централізованою адаптивною маршрутизацією є центральна інстанція, якій усі вузли передають інформацію про завантаженість каналів, наявність черг. На підставі такої інформації ця інстанція розраховує таблиці маршрутизації і пересилає їх усім вузлам мережі. У цьому випадку генерується невеликий додатковий маршрутний трафік. Недоліком централізованої маршрутизації є те, що інформація, яка надходить до вузлів, уже застаріла. Крім того, надійність мережі залежить від надійності сервера централізованої маршрутизації (порівняйте з механізмами виділення адрес службою DHCP у мережах TCP/IP, розділ 13).

• **Гібридна маршрутизація** – це комбінація локально-адаптивної та централізованої. У цьому випадку враховано переваги як локальної, так і централізованої маршрутизацій. Сервер маршрутизації розсилає всім вузлам маршрутні таблиці. Однак у кожному вузлі враховується і наявність вихідних черг. Рішення про передавання приймається на підставі оцінки переваг варіантів локальної та централізованої маршрутизацій.

Бібліографія та джерела

1. *Бертсекас Д., Галлагер Р.* Сети передачи данных. М.: Мир, 1989.
2. *Девис Д., Барбер Д., Прайс У, Соломонидес С.* Вычислительные сети и сетевые протоколы. М.: Мир, 1982.
3. *Мизин И.А., Богатырев В.А., Кулешов А.П.* Сети коммутации пакетов. М.: Радио и связь, 1986.

ПРОТОКОЛИ СЕАНСОВОГО РІВНЯ

Головні функції сеансового рівня. Налагодження сеансу. Процедура прив'язання (bind). Передавання інформації. Керування ресурсами за допомогою передавання повноважень. Керування темпом передавання. Робота в нештатних ситуаціях. Контрольні точки. Контрольні множини. Головні форми розірвання сеансу. Робота в аварійному режимі.

Головним завданням сеансового рівня є організація обміну інформацією між об'єктами прикладного рівня за посередництвом об'єктів рівня відображення. Цей обмін, як звичайно, відбувається як послідовність окремих діалогів – сеансів (звідси й назва цього рівня).

Усі функції сеансового рівня можна розділити на такі три групи:

- функції налагодження або розірвання сеансу;
- функції нормального передавання;
- функції нештатних ситуацій.

11.1. Налагодження сеансу

Під час налагодження сеансу виконують такі операції:

- визначають місце, де є потрібна функція або дані;
- налагоджують зв'язок зі станцією, яка має потрібну функцію або дані; одержують її згоду на проведення сеансу;
- перевіряють, чи мають станції потрібні для взаємодії ресурси: пам'ять, буфери тощо;
- перевіряють станції щодо наявності потрібного програмного забезпечення;
- обмінюються інформацією про протоколи, які використовуватимуться.

Процеси налагодження та розірвання сеансу сильно відрізняються залежно від реалізації. У найпростішому випадку для налагодження сеансу достатньо пари пакетів *Запит на сполучення* та *Підтвердження сполучення*, а для розірвання – *Запит на розірвання* та *Підтвердження розірвання*. У складніших ситуаціях потрібна процедура, яка підтверджує, що запит надходить від повноважного користувача, та дає змогу задати параметри обміну. У цих випадках перед налагодженням сеансу виконується **процедура прив'язання** (bind). Вона розпочинається з того, що сеансові об'єкти обмінюються інформацією про типи протоколів, які використовуватимуться, ресурси сеансу (буферну пам'ять, ємність дискового простору для файлу, модулі програмного забезпечення, потреба шифрування тощо), режими обміну (дуплекс, напівдуплекс), формати інформації, тобто узгоджують параметри передавання. Якщо узгодження досягнуто, то об'єкти обмінюються командами bind, що завершує етап прив'язання. Процедура прив'язання подібна до процедури підписання контракту: спочатку домовляються про всі деталі, потім підписують контракт і починають його виконувати.

Після закінчення процедури прив'язання починається сеанс зв'язку.

11.2. Передавання інформації

Під час передавання інформації можуть виконуватися такі функції:

- відображення та перетворення речень мовами високого рівня або запитів протоколів транспортної підсистеми;
- зіставлення запитів та відповідей на ці запити;
- керування чергами повідомлень та їхньою пріоритетністю;
- поділ повідомлень на частини, якщо вони задовгі для транспортного рівня, та зворотне їх об'єднання;
- робота з порядковими номерами пакетів, якщо транспортна підсистема не забезпечує правильної послідовності їх передавання;
- керування потоком та темпом передавання;
- керування використанням ресурсів;
- розподіл повідомлень на звичайні та термінові.

Під час передавання даних відбувається їхній *розподіл на звичайні та термінові*. Термінові дані потрібні для виконання деяких процедур керування, для їхнього передавання не треба дозволу, їх відправляють поза чергою. У цьому випадку забезпечується ідентифікація блоків даних (визначають, якій станції які блоки належать).

Для *керування використанням ресурсів* під час передавання призначена процедура передавання повноважень. Ця процедура має на меті запобігти конкуренції кількох об'єктів сеансового рівня за захоплення одного ресурсу. Для керування цим процесом вводять поняття *ознаки*.

> ***Ознака** – це атрибут сеансового сполучення, який динамічно призначається в кожен момент часу тільки одному користувачу сеансової служби, що дає йому право користуватися певними ресурсами.*

У кожен момент часу ознака може перебувати у двох станах:

- доступності, у цей час вона призначена для одного користувача, інший може одержати ознаку згодом;
- недоступності для всіх користувачів.

Прикладом дії ознаки є блокування можливості зміни запису бази даних. Під час функціонування об'єкти сеансового рівня можуть обмінюватися ознаками.

Якщо потрібне дотримання *послідовності передавання повідомлень* або довгі повідомлення треба розділяти на частини, то необхідною є нумерація пакетів на сеансовому рівні, а також контроль за послідовністю передавання, що відбувається таким же чином, як у протоколах нижнього рівня.

Керування темпом у сеансовій системі потрібне для ефективної роботи приєднаних до неї пристроїв. Кожен пристрій має свою ефективну швидкість роботи. Наприклад, рядковий принтер характеризується циклом друкування одного рядка. Якщо дані не готові, рядок пропускається. Буфер принтера також має обмежену ємність. Якщо його переповнити, дані будуть втрачені. Крім того, тривалість циклу принтера не є сталою, оскільки деякі процедури потре-

бують більше часу. Це ж властиве й іншим пристроям мережі (дисководам тощо). Загалом, кожне обладнання має свої часові параметри та характеристики доступу, на які треба зважати. Узгоджуються часові параметри під час процедури прив'язання, а під час передавання даних система враховує часові параметри для керування темпом передавання.

11.3. Робота в нештатних ситуаціях

Для забезпечення надійності роботи сеансової підсистеми в нештатних ситуаціях передбачені такі операції та функції:

- контроль за групами операцій (контрольні множини);
- відновлення під час поновлень транспортної підсистеми без розірвання сеансу;
- забезпечення, якщо потрібно, примусового завершення сеансу зі збереженням цілісності даних;
- рестарти з контрольних точок та синхронізація;
- розробка варіантів можливої роботи в ручному режимі в періоди масових відмов.

Розглянемо детальніше головні моменти відновлення сеансу.

Усі відмови та помилки, які виникають на сеансовому рівні, можна розділити на такі, що потребують відміни сеансового прив'язання, та такі, що їх можна нейтралізувати за допомогою невеликих коректив. У першому випадку відновлення виконують системи верхнього рівня, у другому – засоби сеансового рівня. Користувач під час цього процесу може помітити лише деяке уповільнення роботи. Можливість сеансового рівня автоматично відновлюватися характеризує його 'живучість'.

До розірвання сеансу можуть призвести такі серйозні причини:

- стійка апаратна помилка, яку не можна обминути;
- стійка помилка в засобах зв'язку;
- помилка в програмі;
- машини не можуть взаємодіяти внаслідок різної генерації систем;
- по-різному реалізовані рівні відображення та прикладний.

Інші можливі помилки, які не призводять до розірвання сеансу, такі:

- скидання або рестарт транспортної підсистеми;
- втрата, дублювання або спотворення повідомлень;
- перевантаження;
- нестійка апаратна помилка;
- тимчасова нестача ресурсів;
- помилки оператора;
- помилка програми, яка не повторюється.

Ініціатором запуску та виконання процедур відновлення є один з учасників сеансу. Він аналізує причину ситуації, присвоює їй відповідний код та надсилає інформацію відповідальній за відновлення інстанції. Ця інстанція не обов'язково повинна бути одним з учасників сеансу, нею може бути і центральний вузол керування.

Збої та відмови бувають різними. В еталонній моделі використано такий принцип: збої, якщо можливо, повинні бути усунуті засобами протоколів нижніх рівнів. Є збої, які впливають тільки на одне повідомлення або на один сеанс, а є й такі, що призводять до поширення розірвання сеансів та виникнення відмов на всі сеанси вузла або частини мережі. Відповідно до цього є багато різних механізмів контролю та відновлення роботи сеансів.

Повернення в контрольну точку

Для структуризації обміну даними та з метою уникнути відмов користувачі сеансового рівня можуть уводити головні точки синхронізації, які розділяють процес обміну даними на одиниці діалогу. У цьому випадку процес передавання у межах однієї такої одиниці не залежить від передавань в інших. Кожна головна точка синхронізації підтверджується явно. Всередині одиниці діалогу можуть бути проміжні точки синхронізації. Однак їхнє підтвердження необов'язкове (рис. 11.1).

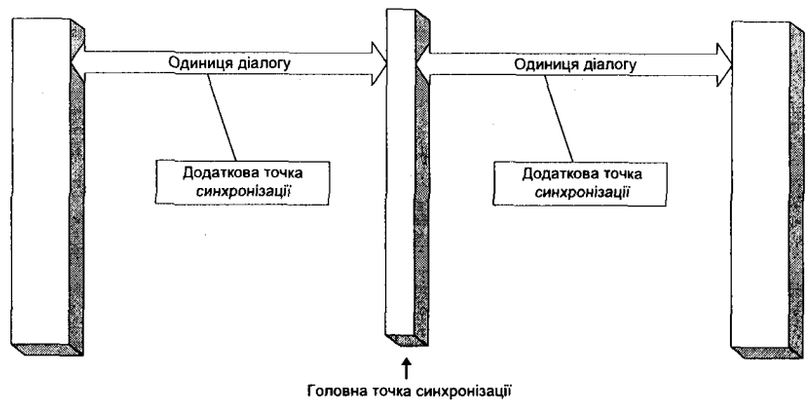


Рис. 11.1. Точки синхронізації.

Контрольна точка – це збережений у деякий момент часу стан даних, прикладної програми та системи керування, який дає змогу деяким попередньо визначеним способом відновити себе. Звичайно контрольна точка – це файл(и) на диску. Контрольні точки зберігаються як на системному рівні (стан мережі в цілому), так і на рівні користувача (під час роботи з базами даних (БД), збереження цілісності БД). Формування нової контрольної точки спричинює знищення старої. Якщо виникає збій, то відбувається повернення в контрольну точку, тобто стан сеансового рівня відновлюється з файлів контрольних точок. Вибираючи частоту формування контрольних точок, враховують цінність інформації та її логічну і фізичну структурованість, а також додаткові витрати часу на формування контрольної точки. Найчастіше контрольну точку формують на кожну транзакцію (наприклад, запам'ятовують стан рахунку в банку до його зміни).

Крім описаних контрольних точок, призначених для уникнення впливу апаратних і програмних збоїв, є й такі, що призначені для контролю та нейтралізації помилок людини. У багатьох діалогових процесах є моменти, коли треба перевірити правильність прийнятих рішень та виконаних операцій, – так звані підсумкові етапи розумового процесу (заповнений документ, зроблене креслення тощо). Тому якщо оператор формує якусь складну послідовність даних, то через деякий час комп'ютер пропонує йому перевірити правильність інформації та зберігає стан роботи.

Контрольна множина – це сукупність даних, що передаються на сеансовому рівні від однієї контрольної точки до іншої, тобто поновлювальна сукупність даних. Контрольну множину вибирають залежно від типу операцій у системі. Наприклад, під час опрацювання документів контрольною множиною може бути одна сторінка, під час роботи з віддаленим файлом – один кластер або запис файлу. За цією сукупністю даних кожен учасник сеансу обчислює контрольну суму, яку згодом порівнюють. Якщо значення збігаються, то діалог відбувся нормально, якщо ж ні, то треба повернутися в контрольну точку.

Для відновлення сеансу потрібно виконати такі дії:

- виявити помилку;
- інформувати відправника про помилку з зазначенням причини;
- виправити помилку, якщо це можливо;
- вибрати контрольну точку та ініціювати процес рестарту.

Як звичайно, помилку виявляє станція приймання. Вона ж інформує про це відправника. Якщо пакет втрачено, то виявити це може і відправник за допомогою тайм-ауту. Найчастіше відповідальною за відновлення сеансу є станція, яка почала передавання. Однак рішення про те, хто буде виконувати відновлення сеансу, приймається під час процедури прив'язання.

Відповідальна за відновлення сеансу станція може таке:

- ресинхронізувати протокол обміну і повторно відправити повідомлення або контрольну множину;
- виправити помилку і після цього повторно відправити повідомлення;
- попросити оператора виправити помилку, наприклад, вкласти папір у принтер;
- вирішити, що автоматичне відновлення неможливе, і розірвати сеанс.

Проста ресинхронізація відбувається, якщо пакет втрачено (закінчився тайм-аут) або відсторонено внаслідок нестачі ресурсів, а також, якщо є помилки в порядкових номерах. Якщо помилка серйозніша, повторно надсилається контрольна множина.

У випадку примусового розірвання сеансу можуть бути зруйновані прикладні програми і дані. Тому, якщо потреба розірвати сеанс усе ж таки виникла, то для мінімізації шкоди розривання виконується акуратно, говорять, що сеанс згортається. Розрізняють м'яке згортання сеансу, а також розриви – напівжорсткі (швидкі) та жорсткі (миттєві).

На прикладному рівні, як звичайно, програми мають спеціальні підпрограми, які очищають буфери, зберігають усі важливі дані так, щоб прикладну програму можна було перезапустити без втрат.

У випадку м'якого згортання сеансу всі прикладні програми мають змогу виконати вихідні підпрограми. Після цього комунікаційна активність припиняється і налагоджувати нові сполучення та передавати нову інформацію не можна. Однак інформація, яка є в чергах на передавання, повинна бути передана.

Під час напівжорсткого розірвання сеансу запускати вихідні програми можна, однак черги повідомлень не опрацьовуються. Можуть бути завершені лише поточні передавання. У випадку жорсткого розірвання припиняються всі операції.

Робота в аварійному режимі

На випадок, коли мережа повністю виходить з ладу, передбачають можливість тимчасової роботи в ручному режимі. Для цього розробляють конкретні процедури та заходи (найчастіше це періодичне роздруковування інформації про стан файлів). Робота в ручному режимі дещо сповільнює виконання функцій, зменшує сервіс, однак головні функції система виконує. Комп'ютери в цьому випадку працюють в автономному режимі.

11.4. Стандарти протоколів сеансового рівня

Для реалізації сеансового рівня не обов'язково виконувати всі функції. Міжнародні стандарти для цього визначають функціональні блоки – логічні набори пов'язаних між собою функцій. Визначено такі блоки: базовий, узгодження вивільнення ознак, дуплексний та напівдуплексний, передавання термінових та службових даних, головної синхронізації, керування діяльністю та ін. На сеансовому рівні обов'язково реалізувати базовий блок, який передбачає функції налагодження та розірвання сеансу, передавання інформації. Вислідні можливості рівня формують комбінацією блоків у систему без протиріч.

Стандарт ECMA-75 визначає чотири класи сервісу для сеансового рівня.

A. Налагодження сполучень, їх ідентифікація. Надсилання підтверджень про цілісність та безпомилковість інформації.

B. Взаємодія з протоколом віртуального термінала. Вибір дуплексної або напівдуплексної форми передавання. Можливість передавання великих неподільних повідомлень.

C. Організація діалогу з синхронізацією для протоколу віртуального файлу. Функції класу **B,** а також забезпечення синхронізації і ресинхронізації. Керування роботою за допомогою передавання повноважень.

D. Визначення спрощеної процедури діалогу для простих прикладних процесів.

Вибір класу сервісу сеансу відбувається під час процедури прив'язання.

Бібліографія та джерела

1. *Девис Д., Барбер Д., Прайс У, Соломонидес С.* Вычислительные сети и сетевые протоколы. М.: Мир, 1982.
2. *Мартин Д.* Вычислительные сети и распределенная обработка данных. Программное обеспечение, методы и архитектура: В 2 т. М.: Финансы и статистика, 1985.

ПРОТОКОЛИ РІВНЯ ВІДОБРАЖЕННЯ ТА ПРИКЛАДНОГО РІВНЯ

Функції та призначення протоколів рівня відображення. Принцип контексту. Функції редагування, забезпечення діалогу, віртуальних операцій та прозорості. Поняття віртуального термінала та віртуальної машини. Функції стиснення, безпеки та контролю. Функції та призначення протоколів прикладного рівня. Макрокоманди на прикладному рівні. Керування програмами. Функції доступу до файлів. Функції оплати.

12.1. Функції та призначення протоколів рівня відображення

Протокол рівня відображення призначений для відображення та перетворення даних у вигляді, зручному для різноманітних прикладних процесів. В основу означення сервісу рівня відображення міжнародні організації зі стандартизації поклали принцип контексту. Контекст – це набір форм опису даних, які використовують у конкретному сеансі передавання. Функції рівня відображення можна умовно розділити на такі групи:

- редагування;
- забезпечення діалогу;
- віртуальних операцій та прозорості;
- стиснення;
- безпеки та контролю.

Функції редагування

До групи функцій редагування належать такі:

- форматування даних відповідно до заздалегідь визначених форматів документів;
- перекодування;
- додавання заголовків, дат, колонтитулів, номерів сторінок тощо.

Для економії пам'яті, надання документам потрібного вигляду, інформацію, яка надійшла від об'єкта рівня відображення, **редагують** за допомогою спеціально закодованого формату. У комп'ютері, який виконує редагування, є багато різних форматів, їх можна вибрати під час налагодження сполучення рівня відображення або динамічно під час сеансу. Код потрібного формату є в заголовках повідомлень протоколу рівня відображення. Одержана інформація перетворюється відповідно до цього формату. Наприклад, текст ділиться на сторінки, формуються абзаци, нумеруються сторінки тощо.

Перекодування потрібне у випадку, коли прикладні процеси, які обмінюються інформацією за допомогою об'єктів рівня відображення, використовують різні коди та команди.

Функції забезпечення діалогу

До групи функцій забезпечення діалогу належать такі:

- збереження кадрів-форматів, що часто використовуються, та виведення їх на екран за допомогою ідентифікаційного коду;
- забезпечення режимів *вибір з меню*, *команда-відповідь* або інших форм діалогу, незалежних від програм використання, з передаванням тільки результату діалогу;
- ведення діалогу, з метою надати користувачу допомогу у формуванні запиту до БД;
- керування операціями збирання та введення даних, підвищення їхньої ефективності.

Головна вимога до проектування діалогових систем – це зробити діалог якнайпростішим та максимально ефективним, тобто досягти швидкої відповіді або швидкого виведення на екран великої кількості символів. Деякі з тих символів є стандартним текстом або шаблоном (кадром-форматом), який може зберігатися на периферії. Замість кадрів-форматів мережею передаються закодовані посилання на них. Кадри, які з'являються на екрані під час діалогу, можуть бути стандартними з деякою частиною змінної інформації. У цьому випадку повідомлення доцільно будувати зі змінної інформації та ідентифікатора кадру-формату.

Аналогічно під час роботи з меню: ціле меню передавати необов'язково, а тільки відповідь – який пункт меню вибрано. Файли допомоги також ліпше розмістити в абонентів, а не передавати їх мережею.

Функції віртуальних операцій та прозорості

До цієї групи функцій належать такі:

- надання можливості звертатися до віртуального термінала. Відображення форматів та сигналів керування віртуального термінала на реальний;
- надання можливості працювати з іншими віртуальними машинами;
- надання можливості використовувати логічні пристрої введення-виведення або зону на екрані дисплея та відображати їх на конкретні фізичні пристрої;
- надання доступу до кількох транспортних систем;
- забезпечення невидимості транспортної системи для користувача.

До інформаційної мережі можна приєднати багато різноманітних терміналів. Усі вони відрізняються процедурами керування, інформаційною місткістю екрану, механізмами та сигналами керування. Оскільки термінали постійно вдосконалюють, то розробники стандартів для протоколів мереж вирішили орієнтуватися на абстрактний (віртуальний) термінал. Для нього визначені процедури керування та поле екрана. Кожному об'єкту рівня відображення треба узгодити свій термінал з віртуальним та перетворювати дані у двох напрямах: свій ⇒ віртуальний та навпаки. Для зручності виділяють кілька типів віртуальних терміналів: дисплей, зчитувач кредитних карток, телекс та ін.

Інколи в користувача мережі може виникнути потреба працювати з якоюсь машиною набором характеристик або операційною системою, яких нема в мережі. У цьому випадку

рівень відображення мережі може виконати *емуляцію* потрібної машини чи системи і задовольнити запит користувача за допомогою роботи з іншими машинами мережі. Аналогічно можна розробити концепцію віртуальної машини: користувач звертається до абстрактної машини з узагальненими можливостями через визначений стандартний інтерфейс; інші функції бере на себе мережа.

Рівень відображення може надавати сервіс з відображення логічних пристроїв уведення-виведення (логічних дисків, принтерів, плотерів, різних серверів тощо). На екрані або в програмі вони можуть мати символьне або графічне позначення (піктограму). Якщо користувач вибере відповідне позначення, то рівень відображення протоколу автоматично ставить йому у відповідність реальний пристрій з використанням таблиць відображення.

Функції стиснення

Ця група об'єднує такі функції:

• перетворення коду з метою зменшити кількість бітів, що передаються (вилучення нулів та пропусків, стиснення інформації, попереднє архівування);

• редагування з метою зменшити довжину повідомлень;

• використання ідентифікаційних кодів для зображень на екрані, форматів, графічних або текстових фрагментів, які повторюються.

Оскільки вартість опрацювання даних зменшується значно швидше, ніж вартість їх передавання, то економічно вигідно стискати дані перед передаванням, щоб зменшити кількість бітів. Цього можна досягти за допомогою попереднього редагування інформації. Однак найчастіше для стиснення використовують різні модифікації алгоритмів Лемпеля-Зіва, оптимальне кодування кодами Хаффмена або Шеннона-Фано. Ступінь стиснення залежить від виду інформації, що передається. Наприклад, графічну інформацію стиснути важко, текстову – значно легше (на 30–40%).

Функції безпеки та контролю

Ця група передбачає виконання таких функцій:

• фільтрація повідомлень, у результаті чого надходять тільки виклики від повноважних користувачів;

• керування доступом: кожна робоча станція або користувач можуть сполучатися тільки з конкретними, заздалегідь визначеними машинами та користувачами;

• ведення БД паролів та їх перевірка ;

• шифрування та дешифрування повідомлень;

• ведення журналу реєстрації подій, за якими можна виявити спроби порушення режиму безпеки.

Є багато способів забезпечити секретність у мережах, зокрема такі: шифрування повідомлень, керування доступом до мережі, обмеження кількості станцій, з якими можна налагоджувати сеанси, перевірка прав користувачів. Можна вести журнали контрольних слідів: де, коли, хто приєднався, скільки працював, з чим і з якою швидкістю тощо.

12.2. Стандарти рівня відображення

Як уже зазначено, міжнародні організації зі стандартизації в основу означення сервісу рівня відображення поклали принцип контексту. Рівень відображення визначає кілька контекстів і дає змогу вибрати той, який потрібний у конкретному сеансі.

Головні види сервісу за ISO такі:

• налагодження та розірвання сполучень на рівні відображення;

• вибір потрібних контекстів;

• передавання форматованої інформації користувачів;

• контроль передавання даних.

Європейська асоціація виробників комп'ютерів розробила такі чотири взаємопов'язані стандарти.

Стандарт ECMA-86 визначає головні принципи відображення даних і координації структури інших стандартів. У ньому:

• наведена термінологія, концепція і модель опису сервісу та відображення даних;

• у загальній формі визначено взаємодію двох об'єктів прикладного рівня, що їх використовують сервіси відображення;

• пояснено спосіб взаємодії прикладних об'єктів та об'єктів відображення.

Стандарт ECMA-84 характеризує функції, потрібні для реалізації протоколу віртуального файлу, а саме:

• сервіс для об'єктів прикладного рівня;

• процедуру виконання сервісу;

• спосіб відображення протокольних об'єктів на сеансовий рівень.

Стандарт ECMA-87 описує протокол узагальненого віртуального термінала, його модель та основні види сервісу. Стандарт задовольняє різні форми роботи різних типів віртуальних терміналів: символьних, графічних, рядкових, сторінкових. З метою охопити всі можливі типи терміналів уведено поняття класу термінала, який визначає набір вимог до його характеристик.

Стандарт ECMA-88 описує базовий (головний) клас відображення віртуального термінала, реальні символьні термінали: рядковий (телетайп), сторінковий (дисплей). Він визначає таке:

• компоненти моделі віртуального термінала;

• види сервісу;

• процедури виконання функцій;

• правила використання сервісу.

Для віртуального термінала визначено чотири основні характеристики:
- вигляд даних, описаних логічною структурою;
- спосіб зміни стану термінала;
- метод сигналізації;
- процедура керування.

12.3. Функції та призначення протоколів прикладного рівня

Протоколи прикладного рівня забезпечують різні форми взаємодії прикладних процесів. На прикладному рівні виділяють такі групи функцій:
- виконання макрокоманд;
- керування програмами;
- функції доступу до файлів;
- функції оплати.

Розглянемо їх детальніше.

Макрокоманди на прикладному рівні:
- виконання макрокоманд у програмах, написаних мовами високого рівня;
- забезпечення прозорості віддаленого розташування інформації. Користувач не повинен знати, де розміщений файл;
- опрацьовування команд прикладної програми, яка використовує віртуальні пристрої;
- виконання мережевих макрокоманд.

Керування програмами:
- завантаження та виконання програм;
- забезпечення можливості обміну програмами між машинами з різними системами команд;
- інтерфейс з мовами керування завданнями операційних систем.

Функції доступу до файлів:
- забезпечення доступу до окремих записів (читання, модифікація, вилучення, доповнення новими записами);
- передавання цілих файлів або їхніх частин;
- вставляння позначок *кінець запису*, *кінець файлу* та їхня інтерпретація;
- переглядання файлу або множини файлів для шукання інформації за ключами;
- виявляння фізичного розміщення даних за символьним посиланням.

Якщо один файл оновлюють одночасно кілька користувачів, то треба використовувати засоби, щоб запобігти взаємним перешкодам і зберегти цілісність даних.

Функції оплати:
- реєстрація ресурсів, які використовують для начислення оплати;
- реєстрація випадків використання програм, текстів, захищених авторськими правами, для начислення гонорару;
- запити на зворотну оплату та відповіді на них.

12.4. Стандарти прикладного рівня

На прикладному рівні ISO рекомендує такі протоколи:

FTAM (File Transmission Application Method) – керування передаванням файлів;

JTM (Job Transmission Method) – передавання завдань;

VTSP (Virtual Terminal Service and Processing) – сервіс віртуального термінала.

В основі передавання та керування файлами є принцип віртуального файлосховища. У цій моделі абстрактно описані структура файлу та його характеристики, означено процедури доступу користувачів до файлів.

Передавання та опрацювання завдань ґрунтуються на віддалених уведенні та виведенні програм з використанням зовнішніх пристроїв віддалених ЕОМ. У цьому випадку користувач повинен знати технічні засоби та мову керування завданнями тієї машини, на яку він передає дані. Вважають, що розробляти єдину мову керування завданнями наразі недоцільно.

Сервіс віртуального термінала призначений для роботи користувачів терміналів з прикладними процесами різних робочих станцій. Форма обміну інформацією – діалог коротких повідомлень. Одним з перших протоколів прикладного рівня був протокол віртуального файлу **ECMA-85**. У ньому означено загальну модель файлу, незалежну від комп'ютера та операційної системи. Сервіс ECMA-85 розподілено на дві категорії:
- правила доступу до віртуального файлу або його частини;
- процедури керування віртуальним файлом.

Адресація файлу дворівнева. Перша адреса визначає ім'я віртуального файлосховища, де є файл, друга – описує ім'я файлу. Далі міститься інформація про захист файлу від несанкціонованого доступу. Для цього протоколом передбачено введення списку осіб, які мають право одержувати інформацію з файлосховища, а також уведення паролів доступу до файлу.

Бібліографія та джерела

1. *Девис Д., Барбер Д., Прайс У., Соломонидес С.* Вычислительные сети и сетевые протоколы. М.: Мир, 1982.
2. *Мартин Д.* Вычислительные сети и распределенная обработка данных. Программное обеспечение, методы и архитектура: В 2 т. М.: Финансы и статистика, 1985.

Розділ 13

ПРОТОКОЛЬНІ СТЕКИ TCP/IP ТА SPX/IPX

Поняття протокольного стека. Протокольний стек TCP/IP, його загальна характеристика. Структура мережі TCP/IP. Адресація. Головні протоколи стека. Формат IP-пакета. Маршрутизація в мережах TCP/IP. Протокольний стек SPX/IPX.

У попередніх розділах ми розглянули функції та призначення протоколів усіх рівнів згідно з еталонною моделлю взаємодії відкритих систем. У реальних мережах часто реалізують цілі набори протоколів, які підтримують усі рівні взаємодії.

Конкретна реалізація набору протоколів називається ***протокольним стеком***.

Найбільш поширені сьогодні протокольні стеки TCP/IP та SPX/IPX. Перший з них використовують у мережах ОС Unix та Internet, другий – у виробах фірми Novell.

13.1. Протокольний стек TCP/IP

Набір протоколів TCP/IPI застосовують у мережах на базі ОС Unix, а також у популярній глобальній мережі Internet. Розробку та супровід цих протоколів виконує IAB (Internet Activities Board) з двома підкомітетами: дослідницьким – (Internet Research Task Force (IRTF)) та інженерним – (Internet Engineering Task Force (IETF)). Інженерний підкомітет також розробляє стандарти мережі TCP/IP – RFC (Request For Comments). Крім того, Internet має структуру, що відповідає за розподіл адрес – NIC (Network Information Center).

Структура мережі протоколу TCP/IP

Щодо структури мережу TCP/IP характеризують як об'єднання локальних мереж[1] (звідси назва Internet, дослівний переклад: міжмережева мережа) (рис.13.1). Окремі локальні мережі сполучені через маршрутизатори. Кожна мережа має унікальну адресу. Комп'ютери в локальній мережі називають **гостами** (host). Вони також мають унікальні адреси.

Оскільки мережа протоколу TCP/IP об'єднує кілька локальних мереж, то в англійській термінології її називають ***internet****. (На відміну від всесвітньовідомої глобальної мережі* ***Internet****, яка теж використовує протоколи TCP/IP). Велику корпоративну мережу,*

[1] Поняття локальної мережі тут відображає ступінь зв'язності станцій мережі, їхню функціональну єдність.

побудовану за принципами та на програмному забезпеченні ***internet****, називають* ***intranet****, а таку ж корпоративну мережу, однак з великим ступенем взаємодії з зовнішніми мережами, –* ***extranet****.*

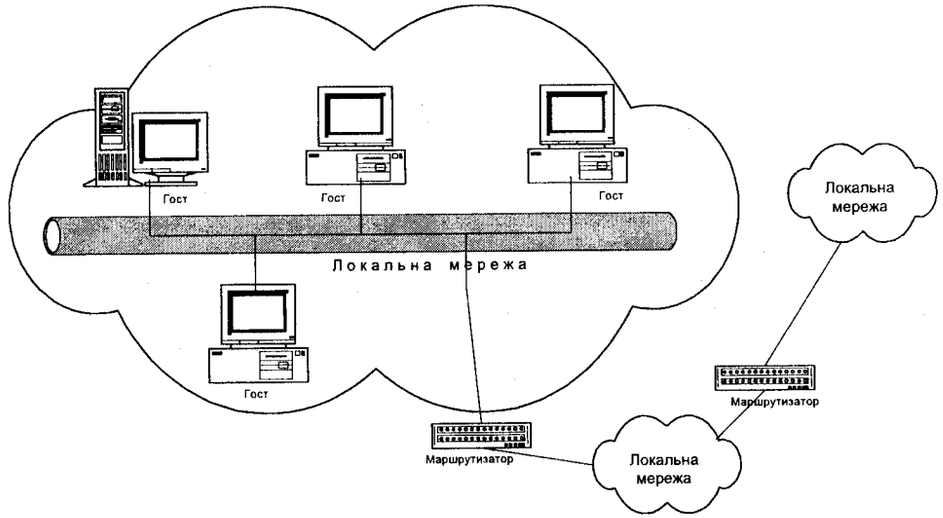


Рис. 13.1. Структура мережі протоколу TCP/IP.

Адресація в мережах протоколу TCP/IP

У кожній мережі на кожному рівні протоколу є свій механізм адресації. Наприклад, у мережі Ethernet на канальному рівні адресу задають унікальним шестибайтовим числовим значенням (наприклад, 08-000-14-57-69-69). IP-адреса (тобто адреса протоколу IP мережевого рівня) вузла також є унікальною логічною адресою і не залежить від апаратури та конфігурації мережі, її довжина становить 4 байти. Для зручності та наочності цю адресу розділяють на чотири частини, відокремлені крапками. Наприклад, 102.54.94.97.

Кожна IP-адреса складається з двох компонент: адреси локальної мережі та адреси госта. Межа між адресами локальної мережі та госта – рухома. Адреса мережі може займати 3, 6, 9 розрядів. Решта – це адреса госта в мережі.

Отже, адреси всіх гостів в одній локальній мережі відрізняються тільки в частині 'адреса госта'.

Для зручності адресації мереж різних розмірів їх було розділено на класи (табл.13.1, рис. 13.2).

Таблиця 13.1. Класи мереж internet

Клас	Значення першого байта	Формат адреси мережі	Формат адреси госта	Кількість мереж	Кількість гостів
A	1-126	w	x.y.z	126	16.777.214
B	128-191	w.x	y.z	16.384	65.534
C	192-223	w.x.y	z	2.097.151	254

Для зручності визначення адреси локальної мережі за IP-адресою ввели поняття *маски мережі*. **Маска мережі** – це чотирибайтове число, за формою запису подібне до IP-адреси. Бітам, що описують мережу, відповідають '1' маски, а бітам адреси госта – '0'. Наприклад, для адреси 192.168.45.1 маска мережі мала б бути 255.255.255.0. Іншим застосуванням масок мереж є поділ мереж на менші підмережі з метою ефективного використання адресного простору.

Адреси з номером мережі 127 зарезервовані для тестової перевірки наявності зв'язку з собою (loopback) та перевірки функціонування міжпроцесних зв'язків. Адреси мереж з номерами 224 і більше призначені для спеціальних протоколів, їх не можна використовувати для адрес станцій.

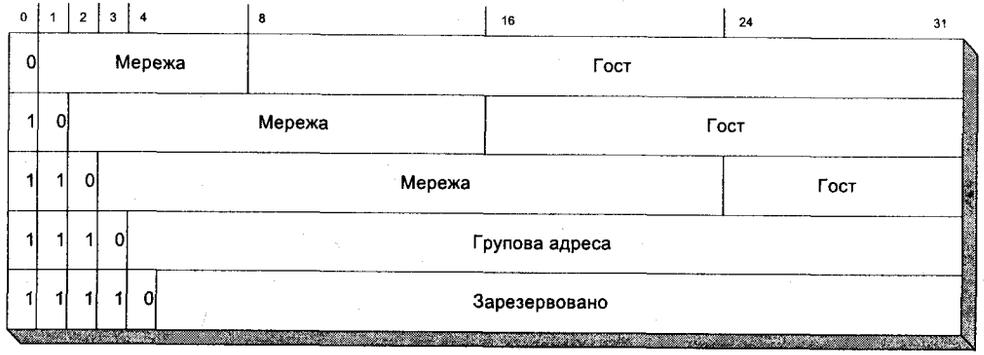


Рис. 13.2. Структура адреси.

Схемою адресації TCP/IP передбачено передавання групових та циркулярних повідомлень. **Групові повідомлення** (Multicast messages) передаються згідно з адресою класу D всім гостам певної групи за допомогою протоколу **IGMP** (Internet Group Management Protocol) (див. Д.13.1). Інформація про станції-члени груп є в таблицях маршрутизаторів. **Циркулярні повідомлення** (Broadcast Messages) передаються всім станціям локальної мережі.

Для зручності користувачів кожна станція мережі, крім IP-адреси, має і своє унікальне в межах конкретної мережі символьне ім'я (DNS-ім'я), яке складається з імен комп'ютера та домену (ширшої зони, яка відповідає організації, країні або типу організації, до якої належить

мережа). Наприклад, ім'я x.acme.com визначає комп'ютер з назвою x у локальній мережі фірми acme, що є комерційною організацією.

Для взаємно однозначного відображення між числовим форматом IP-адреси та його символьним зображенням у мережі TCP/IP може функціонувати ***служба імен DNS*** *(Domain Name System). Про DNS та інші служби імен див. Д.13.2.*

Довжина IP-адреси (4 байти) та пов'язане з цим обмеження кількості мереж сьогодні не дають змоги мережі Internet зростати. Тому розроблено декілька пропозицій щодо збільшення довжини IP-адреси. Одна з них описана в Д.13.3.

Структура протокольного стека TCP/IP

Розглянемо структуру протокольного стека TCP/IP (рис. 13.3) та коротко схарактеризуємо кожен з протоколів.

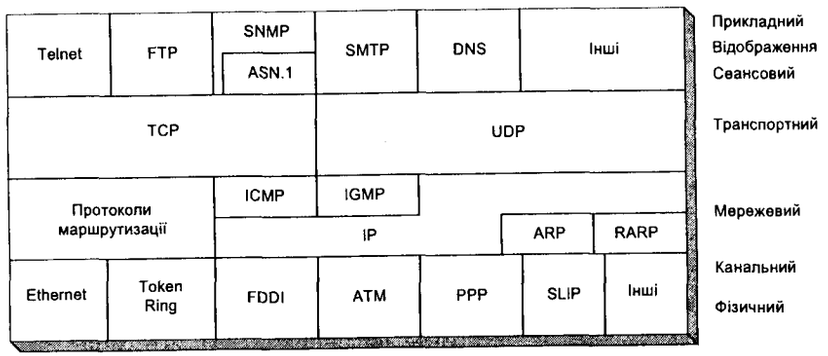


Рис. 13.3. Структура стека протоколів.

На канальному рівні використовують протоколи відомих мережевих архітектур (Ethernet, FDDI, ATM, Token Ring та ін.). Особливе місце посідають протоколи **SLIP** (Serial Line IP) та **PPP** (Point To Point Protocol). Їх застосовують для передавання даних низькочастотними послідовними каналами, найчастіше через послідовний порт комп'ютера та модем призначеною або комутованою телефонною лінією (див. Д.13.4).

IP (Internet Protocol) – це міжмережевий дейтаграмний протокол мережевого рівня, що забезпечує сервіс передавання пакетів між вузлами мережі. Він не підтримує функції послідовного передавання пакетів та не гарантує надійності їх передавання. IP є основним протоколом мережевого рівня стека TCP/IP. Його використовують усі інші протоколи.

ICMP (Internet Control Message Protocol) – це основний діагностичний протокол для передавання інформації між вузлами мережі про помилки та збої, а також для діагностування мережі. Крім того, протоколи верхніх рівнів використовують його для адміністрування та діагностування мережі (див. Д.13.5).

ARP (Adress Resolution Protocol) трансформує IP-адресу в канальну адресу станції (див. Д.13.6), а протокол **RARP** (Reverse Adress Resolution Protocol) виконує зворотну функцію – за канальними адресами визначає логічні IP-адреси.

Кожен IP-пакет містить IP-адреси відправника та одержувача. Водночас для правильного передавання пакета на канальному рівні (у пакеті є канальні кадри) відправник повинен знати і канальну адресу одержувача. Якщо ж канальна адреса одержувача невідома, то IP розсилає спеціальний пакет запиту – ARP Request Packet – з зазначенням IP-адреси вузла, з яким треба налагодити зв'язок. Цей запит приймуть усі вузли, де діє протокол ARP, а вузол, чия IP-адреса наведена в запиті, повідомить свою канальну адресу. Вузол-відправник одержить це повідомлення, скоректує свої таблиці і в подальшому буде користуватись інформацією з них.

TCP (Tramsmission Control Protocol) є протоколом транспортного рівня з попереднім налагодженням сполучення. Він гарантує надійне передавання пакетів та забезпечує їхню правильну послідовність, під час передавання використовує сервіс протоколу IP (див. Д.13.7).

UDP (User Datagram Protocol) – даграмний протокол транспортного рівня, який використовують замість протоколу TCP, якщо немає потреби в додаткових заходах щодо забезпечення надійного передавання. Протокол не гарантує передавання пакета, а також послідовності передавання (див. Д.13.8).

Серед протоколів прикладного рівня та рівня відображення можна виділити **Telnet** – протокол емуляції термінала, **FTP** (File Transfer Protocol) – протокол передавання файлів, **SMTP** (Simple Mail Transfer Protocol) – протокол електронної пошти (Д.13.9), **SNMP** (Simple Network Management Protocol) – протокол керування мережею, **DNS** (Domain Name Service) – протокол служби логічних імен.

Протоколи стека TCP/IP не пристосовані для передавання ізохронних інформаційних потоків, які широко використовують сучасні застосування мультимедіа. Вчені запропонували декілька протоколів для опрацювання ізохронних потоків (див. Д.13.10).

Структура IP-пакета

IP-пакет складається з заголовка, який переносить службову інформацію, та блоку даних. Його структуру (RFC-791) показано на рис. 13.4.

Рис. 13.4. Структура IP-пакета.

Структура заголовка зображено на рис. 13.5. Як бачимо, заголовок складається з окремих полів. Розшифруємо їхнє призначення детальніше.

VERS – номер версії протоколу IP. Його використовують для вирішення конфліктів у випадках, коли станції працюють з різними версіями протоколу IP. Це єдине незмінне поле у форматі пакета.

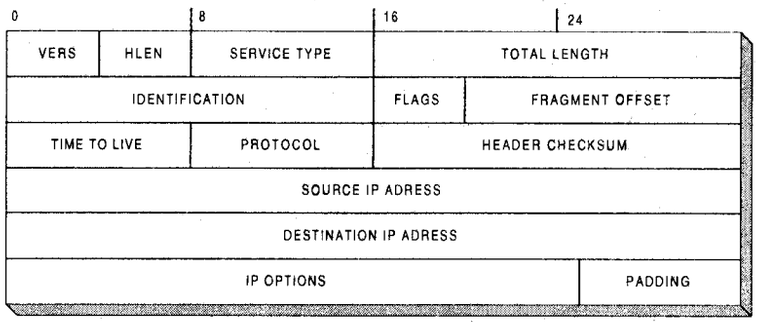


Рис. 13.5. Структура заголовка IP-пакета.

HLEN – довжина заголовка.

SERVICE TYPE – байт, який визначає параметри обслуговування пакета. Біти 0–2 у ньому задають пріоритет пакета, біти 3–6 – бажаний тип якості транспортування (Delay, Throughput, Relability, Cost). Значення пріоритету змінюються від 0 (найнижчий, звичайні повідомлення) до 7 (найвищий, мережеве керування). Тип якості транспортування враховують багато маршрутизаторів. У цьому випадку вони намагаються мінімізувати (максимізувати) відповідний параметр. Одночасно можна задати тільки один з бітів якості. Значення за замовчуванням – усі нулі. Кожна з програм рівня застосувань може ставити свої вимоги до якості передавання. Наприклад, для програми емулятора термінала telnet важливим є час відповіді, а для протоколу мережевого керування SNMP – надійність доставляння.

TOTAL LENGTH – загальна довжина пакета в байтах. Максимальне значення – 65535 байтів.

IDENTIFICATION – ідентифікатор 'великого' пакета, один для всіх його фрагментів.

Під час передавання по internet IP-пакет проходить через багато комп'ютерних систем, кожна з яких має обмеження – максимальний розмір кадру (Maxitum Transfer Unit – MTU). Тому, щоб передати інформацію у систему з меншим розміром кадру, великі пакети доводиться розділяти на менші, а потім знову об'єднувати їх. Оскільки ж деякі апаратні пристрої не можуть правильно фрагментувати та дефрагментувати пакети, то у мережі TCP/IP виникають збої.

FLAGS – ознака того, що пакет фрагментовано.

FRAGMENT OFFSET – зміщення від початку фрагментованого пакета.

TIME TO LIVE – час перебування пакета в мережі. Введення такого параметра дає змогу уникнути необмеженого в часі перебування пакета в мережі. Для цього під час формування пакета йому присвоюють конкретний час. Пізніше у разі кожного опрацювання пакета в

маршрутизаторі цей час зменшується. Коли значення поля досягне 0, пакет знищується. На практиці замість часу перебування часто використовують ціле число – максимальну кількість транзитних маршрутизаторів і в разі кожного опрацювання пакета зменшують його на 1.

PROTOCOL – протокол транспортного рівня, якому спрямований пакет (TCP, UDP, ICMP, IGMP).

HEADER CHECKSUM – контрольна сума, яка захищає заголовок пакета.

SOURCE IP ADRESS – адреса джерела інформації.

DESTINATION IP ADRESS – адреса призначення.

ID OPTIONS – необов'язкові параметри, пов'язані з режимами безпеки та маршрутизацією (детальніше див. Д.13.10).

PADDING – заповнення пропусками до цілого числа 32-бітових слів.

Маршрутизація в мережах TCP/IP

Як уже зазначено, мережа TCP/IP складається з локальних мереж, сполучених маршрутизаторами (routers) (рис. 13.6). У маршрутизаторах є інформація про локальні мережі, приєднані до internet.

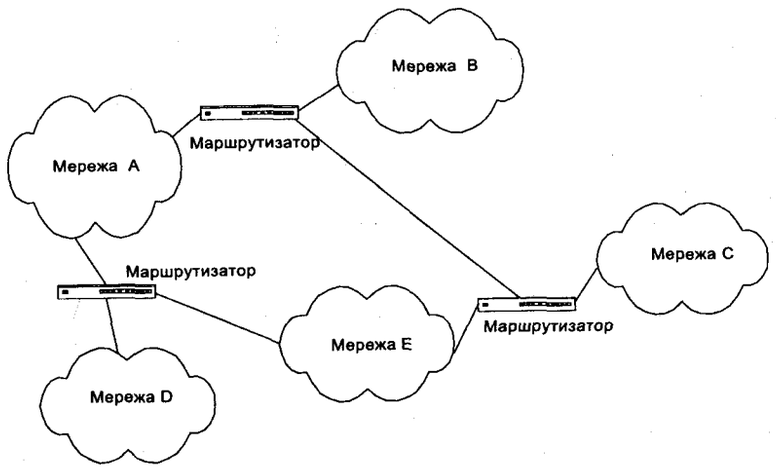


Рис. 13.6. Маршрутизація в мережі TCP/IP.

Кожен гост мережі може підтримувати статичну маршрутизацію. Для цього він має спеціальний файл, у якому зазначено маршрут передавання пакета для конкретних адрес призначення. Під час підготовки пакета до передавання в його заголовок записують адреси джерела та призначення. Якщо адреси локальних мереж у них збігаються, то пакет передається в межах цієї ЛМ, в іншому випадку перевіряється файл статичної маршрутизації на гості. Якщо ж і тут

маршруту з'ясувати не вдалося, то пакет передається на розташовану у тій же ЛМ станцію, адреса якої в параметрах конфігурації госта записана як 'шлюз за замовчуванням' (Default gateway). Таким шлюзом (фактично маршрутизатором) є комп'ютер, де зберігаються таблиці, за допомогою яких, якщо відома адреса призначення пакета, можна визначити адресу іншого маршрутизатора або локальної мережі. Шлюз спрямовує одержаний пакет на таким чином визначену адресу.

У файлі конфігурації станції можна задати декілька адрес маршрутизаторів за замовчуванням. Якщо один з них не працює, то станція звертається до іншого.

Важливим у маршрутизації є поняття автономної системи. **Автономна система** (АС) – це комплекс з однієї або кількох мереж, сполучених маршрутизаторами, у якому підтримується єдиний тип маршрутизації. Маршрутизація всередені АС називається *внутрішньою*, а з виходом назовні – *зовнішньою*. Маршрутизатори АС мають повні маршрутні таблиці для внутрішньої маршрутизації. Якщо ж пакет потрібно передати у зовнішню систему, то його надсилають так званому **граничному маршрутизатору** (Border Gateway). Звичайно він розташований на межі автономної системи і його таблиці містять інформацію як про мережі АС, так і про зовнішні мережі. Використання граничних маршрутизаторів дає змогу зменшити розміри таблиць внутрішніх маршрутизаторів і підвищити ефективність їхньої роботи. Складні АС можна поділяти на області, сполучені граничними маршрутизаторами. Використання АС дає змогу застосувати принцип обмеження потоку, реалізований у ЛМ для їх об'єднання.

Протоколи маршрутизації бувають статичними та динамічними. У статичних протоколах зміни робить адміністратор мережі, у динамічних це відбувається автоматично.

Детальніше проблеми маршрутизації в мережах TCP/IP, а також протоколи внутрішньої (RIP, OSPF) та зовнішньої (BGP) маршрутизації розглянуто в Д.13.11–Д.13.15.

13.2. Протокольний стек SPX/IPX

Загальна характеристика

Протокольний стек SPX/IPX широко використовують у популярних мережах Novell Netware. Подібно до протоколів стека TCP/IP, протоколи SPX/IPX орієнтовані на сполучення як в окремих локальних мережах, так і в їхніх об'єднаннях (мережі класу internet). У SPX/IPX застосовують протоколи та вирішення протокольних архітектур фірми Xerox. Протоколи SPX/IPX визначені як міжмережеві транспортні та данограмні.

IPX (Internet Datagram Protocol) – це простий данограмний протокол мережевого рівня, що не гарантує передавання пакета адресатові. Формат IPX-пакета збігається з форматом пакета міжмережевої данограми фірми Xerox (див. розділ 9).

SPX (Xerox Sequenced Packet Exchange) грунтується на протоколі IPX, а також забезпечує надійне передавання пакетів та послідовність їх надходження. У SPX-пакеті до IPX-пакета додається 12-байтне поле керування.

Схема адресації

Схема адресації SPX/IPX визначена групою мережевих систем фірми Xerox. Адреса складається з таких частин: адреса гост-системи (48 біт); номер мережі (32 біти); номер порту (16 бітів).

Номер порту ще називають номером гнізда (socket). Він ідентифікує процес верхнього рівня, якому призначено пакет (порівняйте зі схемою адресації міжмережевого протоколу Xerox, розділ 9).

Алгоритм маршрутизації Netware

Алгоритм маршрутизації Netware є повністю розподіленим. Процеси прийняття рішень щодо маршрутизації відбуваються в багатьох вузлах мережі (у маршрутизаторах та серверах Netware). Алгоритм реалізується двома процесами:

- вимірювання та ідентифікації (простежуються зміни топології та стану мережі);
- розповсюдження маршрутної інформації.

Маршрутизатор реєструє кількість проміжних вузлів між ним та іншими маршрутизаторами та час надходження до них інформації. Сервери та маршрутизатори стежать один за одним шляхом періодичного надсилання один одному інформації про свій стан.

Під час ініціалізації маршрутизатор опитує інші маршрутизатори про їхній стан, після чого періодично розсилає циркулярні повідомлення про мережі та маршрутизатори, щодо яких він має маршрутну інформацію. Маршрутна інформація складається з номера локальної мережі, віддаленості її від маршрутизатора та приблизного часу передавання пакета, що має 576 байт, від маршрутизатора до цієї мережі. Інформація про зміни в таблиці маршрутизації негайно передається на всі інші маршрутизатори мережі. Якщо інформація про якийсь сервер або мережу втрачається, маршрутизатор шукає альтернативні шляхи передавання даних та повідомляє про це інші маршрутизатори.

Бібліографія та джерела

1. *Гусак О.* Какой курьер лучше? // Компьютеры+программы. 1998. № 2 (44).
2. *Крейг Х.* Персональные компьютеры в сетях TCP/IP. К.: BHV, 1997.
3. *Люис К.* Качество обслуживания, или как добиться неравенства в мире равноправия // Сети и системы связи. 1977. № 11.
4. *Пьянзин К.* Система доменов Internet // LAN Magazine: Русское издание. 1997. № 3.
5. *Семенов Ю.А.* Протоколы и ресурсы Internet. М.: Радио и связь, 1996.
6. *Сталлингс У.* RTP и RSVP: доставка в срок // LAN. 1997. № 5.
7. *Хелд Г.* IP для нового поколения // LAN. 1997. № 5.
8. *Холл Е.* Тонкая настройка DNS // Сети и системы связи. 1997. № 1.

ДОДАТКИ ДО РОЗДІЛУ 13

Д.13.1. Підтримка роботи груп (протокол IGMP)

У мережах протокольного стека TCP/IP у деяких випадках потрібно реалізувати груповий (multicast) режим передавання. Цю проблему вирішують за допомогою протоколу IGMP (базового, на рівні локальної мережі) та протоколів DVMRP, MOSPF, PIM для міжмережевих передавань.

Передумови реалізації режиму групового передавання:

- певна кількість IP-адрес (від 224.0.0.0 до 239.255.255.255) виділена спеціально для адресування груп; групова адреса складається з префікса 1110 та ідентифікатора групи; виділяє групові мережеві адреси **IANA** (Internet Assigned Numbers Authority);
- групову адресацію можна реалізувати і на канальному рівні (наприклад, Ethernet та FDDI її підтримують); для підтримки групового передавання IANA має блок Ethernet-адрес, який починається з 01-00-5E. Під час передавання протокольних блоків між рівнями відбувається копіювання молодших 23-х бітів IP-адреси у хвіст Ethernet-адреси.

У випадку передавання в межах однієї локальної мережі адаптер трансформує групову IP-адресу у групову Ethernet-адресу.

Протокол IGMP регламентує обмін між гостом та маршрутизатором локальної мережі. Якщо до мережі приєднано кілька маршрутизаторів, то один з них (що має меншийномер-IGMP v2) стає головним.

IGMP має кілька версій. Базовою є RFC-1112. Згідно з нею маршрутизатор періодично генерує циркулярні повідомлення HMQ (Host Membership Query) з адресою призначення 224.0.0.1 і полем *TTL*=1. (Отже, цей пакет не може вийти за межі ЛМ). Якщо гост одержав HMQ, він відповідає пакетом HMR (Host Membership Report) кожній групі, членом якої він є. У цьому випадку гост аналізує появу аналогічних повідомлень від інших гостів його групи та відкладає передавання. Таким чином регулюється трафік.

Пакети IGMP передаються всередини IP-пакета. Структура IGMP-пакета показано на рис. Д.13.1.1.

Рис. Д.13.1.1. Структура IGMP-пакета.

Для підтримки діяльності групи маршрутизатор повинен одержати повідомлення від одного госта групи. Він не веде списку гостів груп. Якщо відповіді на декілька запит HMQ немає, то групу вилучають зі списку. Якщо ж гост хоче стати членом якоїсь групи, то він надсилає HMR за своєю ініціативою. Таким чином реєструється група, якщо гост у ній перший.

У випадку, якщо групове передавання треба реалізувати в межах internet-мережі, використовують протоколи DVMRP, MOSPF, PIM. У цьому випадку можна реалізувати радіальне розсилання або алгоритми побудови залишкових дерев (подібні до алгоритмів роботи комутаторів, див. розділ14).

Д.13.2. Служба імен DNS

Адресу госта мережі internet, як уже зазначено, можна записати як за допомогою цифр, так і літерами, що надає їй змістовності, поліпшує запам'ятовування та опрацювання людьми.

Системи іменування мережевих об'єктів поділяють на пласкі та ієрархічні. У пласких системах кожен комп'ютер має текстовий файл (наприклад, /etc/hosts), у якому символьні імена відповідають цифровим IP-адресам. Ідентичні копії такого файлу повинні бути у всіх гостах локальної мережі. Однак зі збільшенням мереж узгоджувати текстові файли стало важче.

У середині 80-х років науковці розробили гнучкішу ієрархічну доменну систему іменування DNS. Головною структурною одиницею у ній є домен. Домени побудовані у вигляді ієрархічного дерева (рис. Д.13.2.1), у вершині якого є кореневий домен '.'. Домени першого рівня відповідають типам організацій, або країнам, наприклад, com – комерційні, int – міжнародні, mil – військові, net – мережеві агентства та провайдери, de – Німеччина, ua – Україна.

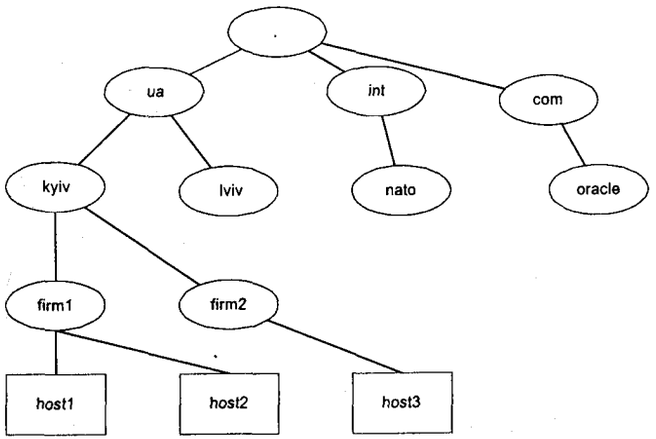


Рис. Д.13.2.1. Дерево доменів.

Довільний домен або гост характеризується повним доменним ім'ям (Fully Qualified Domin Name (FQDN)). Окремі частини імені відділені крапкою. Наприклад, для госта host1 ім'я буде таке:

host1.firm1.kyiv.ua.

Ознакою повного доменного імені (та наявності кореневого домена) є остання крапка.

Адресація за повним доменним ім'ям є **абсолютною доменною адресацією**. Крім абсолютної, використовують і **відносну доменну адресацію**, зокрема, якщо звертаються до комп'ютера в межах одного 'старшого' домену. Наприклад, host1 може звертатися до host2 за адресою host2. У відносній доменній адресі немає кінцевої крапки і вона автоматично доповнюється до абсолютної адреси додаванням адреси 'старшого' домену. В деяких реалізаціях протоколу TCP/IP вважають: якщо в адресі більше одної позначки доменів – то це абсолютна адреса.

DNS – це розподілена база даних, окремі частини якої зберігаються на комп'ютерах – серверах імен. У кожному сервері є інформація тільки про частину загального дерева DNS, а також, обов'язково, посилання на сервери імен, що зберігають інформацію про суміжні частини цього дерева. Сервер імен, як звичайно, відповідає не за один домен, а за декілька суміжних, або їхні частини (zone of authority).

У кожній зоні може бути визначено декілька типів серверів DNS:

- **первинний сервер імен** (Primary Name Server) є центральним сховищем інформації про домен;
- **вторинний сервер імен** (Secondary Name Server) зберігає копію інформації з первинного сервера, розвантажуючи його. Копії періодично узгоджуються;
- **сервери для кешування** (Cache only server) зберігають кешовану інформацію, щоб зменшити навантаження на сервери.

У кожному домені для гарантування надійності повинно бути принаймні два сервери (первинний та вторинний).

Інформація, в тому числі одержана від інших серверів DNS, зберігається у кеш-пам'яті. Визначено максимальну тривалість зберігання інформації у кеш-пам'яті і, отже, періоди її оновлення з первинного сервера, оскільки всі зміни спочатку відбуваються там. Інші сервери оновлюють інформацію шляхом її читання після вилучення з кеш-пам'яті.

Програма, яка реалізує функції DNS на ПК клієнта, називається клієнтом DNS. Клієнт може взаємодіяти з сервером DNS у *нерекурсивному* або *рекурсивному* режимах. Розглянемо це на такому прикладі. Клієнт звертається з запитом до сервера DNS щодо з'ясування IP-адреси. Якщо цей сервер відшукає потрібну інформацію у власній зоні або кешованих даних, перданих іншими серверами, він надсилає її клієнту. Якщо ж такої інформації не виявлено, то сервер надсилає адресу іншого сервера DNS, що розміщений ближче до домену, щодо якого одержано запит. Клієнт DNS сам виконає запит до цього домену. Такий режим називається *нерекурсивним*. У *рекурсивному* режимі запит до іншого сервера DNS виконує не клієнт, а сервер DNS, який одержав запит.

Найчастіше використовують нерекурсивний режим взаємодії, оскільки в цьому разі менше завантажений сервер DNS, а також можна ліпше простежити за проходженням запитів.

Налаштування DNS зберігає у файлах /etc/resolv.conf (Unix), etc\resolv.cfg DOS), sys:etc\resolv.cfg (netware), а у Windows NT та Windows 95 – у реєстрі.
Формат файлу resolv.conf такий:

```
domain      firm1.kyiv.ua
name_s1     143.150.180.1
name_s2     143.150.180.4
```

Звичайно, першим зазначають вторинний сервер, потім первинний (для розвантаження). Якщо наявний файл конфігурування DNS, то спочатку шукання імен відбувається на серверах DNS, а якщо там їх не знайдено, то у файлі hosts. Для пришвидшення роботи ліпше звертатися до абонента безпосередньо за IP-адресою.

Головне призначення служби імен DNS – це надавання IP-адрес на підставі символьного доменного імені госта. Для невеликих мереж це вирішують за допомогою текстового файлу hosts або lmhosts на кожній робочій станції

Однак, фактично DNS має значно більші можливості, ніж просте відображення адрес. DNS – це база даних про стан госта. Вона є прообразом служби каталогів мережі, хоч і не виконує всіх потрібних для служби каталогів функцій.

База DNS складається з записів. Кожен запис має тип. Деякі типи записів наведені у табл. Д.13.2.1.

Таблиця Д.13.2.1. Типи записів бази DNS

Тип	Зміст	RFC	Примітка
A	IP- адреса госта	1035	IP-адреса > - символьна адреса
CNAME	Канонічне ім'я домену	1035	Присвоєння довгим символьним іменам коротких псевдонімів
GPOS	Географічне розташування	1712	
HINFO	Процесор та ОС госта	1035	
MX	Ім'я госта або домену переадресування пошти		Переадресування електронної пошти на іншу станцію
TXT	Довільний текст		

Наведемо приклад використання записів формату MX:

```
abc.com     MX  10  sysnt
            MX  20  sysunix
sysnt       MX  10  sysnt
            MX  20  sysunix
sysunix     MX  10  sysunix
            MX  20  sysnt
```

Як бачимо, є три машини: abc.com, sysnt, sysunix. Записи з вищим пріоритетом 10 задають поштовий сервер за замовчуванням. Якщо він недоступний, то пошта надходить на сервер з меншим пріоритетом.

Службу імен мають не тільки мережеві системи протоколу TCP/IP, а й інші (наприклад, СКБД Oracle). Головне завдання, яке ця служба виконує, – це зіставлення мнемонічних команд певного формату, які задають мережевий ресурс, до його мережевої адреси незалежно від типу мережі.

Д.13.3. Протокол IPv6

Як уже зазначено, обмеженість IP-адреси та дефіцит адресного простору сьогодні є важливою проблемою, вирішення якої потребує переходу на нову версію протоколу IP. Згідно зі

статистичними даними та розрахунками, останню доступну IP-адресу буде зайнято в період між 2005–2010 роками. Крім того, протокол IP не забезпечував надійного захисту інформації, не був пристосований до ізохронного передавання. Це спонукало дослідників розпочати (з кінця 80-х років) розробку нових версій IP. У 1995 р. IETF у RFC-1752 опублікував рекомендації щодо протоколу IP наступного покоління.

Відмінності протоколу Ipv6 від Ipv4

• Розмір адреси розширено з 32 до 128 біт. Отже, загальний адресний простір тепер становить 2^{128} гостів (до 1 квадрильйона гостів в 1 трильйоні мереж).

• Спрощено IP-заголовок (рис. Д.13.3.1).

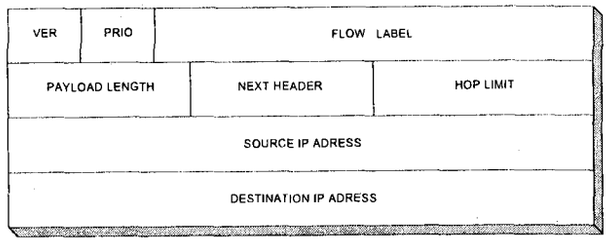


Рис. Д.13.3.1. Структура IP-заголовка.

Спрощення заголовка дає змогу зменшити тривалість опрацювання пакета маршрутизатором. У попередній версії кожен проміжний маршрутизатор, що був на шляху пакета, аналізував записи в полі *Опції*, а також записував туди свою адресу та часову позначку. Новою версією протоколу передбачено, що маршрутизатор аналізує заголовок тільки тоді, коли у полі адреси призначення головного заголовка виявить якусь зі своїх адрес .

Порівняння заголовків IPv4 та IPv6

Поле *Ver* єдине залишилося таким, як у попередній версії. Воно визначає до якого протоколу належить пакет. Замість поля *Total length* довжину пакета визначає поле *Payload Length*, однак, на відміну від старої версії, воно не враховує довжини заголовка. Поле пріоритету *Prio* не тільки дає змогу визначити пріоритет пакета, й поділяє пакети на дві категорії. Пакети першої категорії (значення 0–7) маршрутизатори можуть затримувати, якщо виявлено перевантаження, а пакети другої (8–15) – ні. Отже, другу категорію пріоритетів використовують для передавання ізохронної інформації. Поле *Flow Label* ідентифікує пакети, які маршрутизатор повинен опрацьовувати за допомогою спеціальних процедур. Цю інформацію також використовують для передавання ізохронних даних. Замість поля *Protocol* у новій версії з'явилося багатофункціональне поле *Next Header*. Воно ідентифікує тип наступного після головного заголовка, або тип транспортного пакета. Отже, у новій версії протоколу можна будувати ланцюжки заголовків різних типів (рис. Д.13.3.2).

Визначено шість типів заголовків:

- опису транзитних вузлів (використовують для діагностування, трасування);
- інформації для одержувача (визначає, які дії користувач повинен виконати);
- маршрутизації (список проміжних вузлів);
- відомості про фрагменти (дають змогу дефрагментувати пакети);
- ідентифікації (дає змогу ідентифікувати відправника, розпізнавання пакета);
- кодування (містить відомості про кодування інформаційної частини пакета та його параметри).

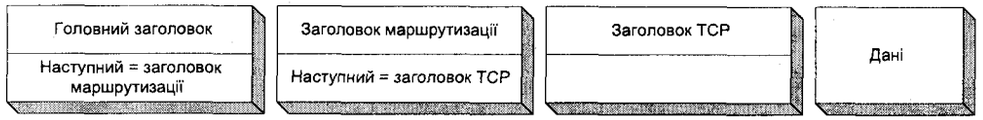


Рис. Д.13.3.2. Послідовність заголовків.

Адресація

Як і в попередній, у новій версії визначено *індивідуальні* (unicast), *групові* (multicast) та *циркулярні* (broadcast) адреси, а також з'явилася *нечітка* адреса (anycast). Пакет, адресований на нечітку адресу, передається найближчому госту вказаної групи. Це зумовлює гнучкість конфігурування мережі. Якщо один з серверів мережі стає недоступним, то пакети відразу ж спрямовують іншому аналогічному серверу без ручного переналаштування.

Клас мережі, як і раніше, визначається двійковим префіксом. В Ipv6 адресу записують як вісім 16-розрядних чисел, розділених двокрапками. Наприклад:

502C:0000:0000:0000:1ACF:00FD:2145:0101.

Записуючи адресу, можна зменшити кількість нулів: опустити початкові нулі, або записати *послідовність нулів* як ::. Наприклад:

502C:0:0:0:1ACF:00FD:2145:0101,
502C::1ACF:00FD:2145:0101.

Д.13.4. Протоколи SLIP та PPP

Протоколи SLIP та PPP призначені для передавання даних низькочастотними послідовними каналами.

Протокол **SLIP** (RFC-1055) уперше був використаний в ОС UNIX 4.2 BSD у 1984 р. Швидкість передавання даних, як звичайно, не перевищує 19.2 Кбіт/с. Максимальний розмір блоку – 256–512 байт. Навіть під час передавання 1 байта накладні витрати перевищують 40 байт. Цей недолік частково усунено в новій версії CSLIP (Compressed SLIP), де заголовок займає 3–5 байт. SLIP інкапсулює IP данограми для передавання послідовними каналами.

Є такі додаткові обмеження використання SLIP:

- кожен партнер обміну повинен знати IP-адресу іншого партнера;
- SLIP не використовує контрольних сум, а функції виправляння помилок переносяться на протокол верхнього рівня;
- кадр SLIP не має поля типу протоколу, що унеможливлює його використання у багатопротокольних мережах.

Протокол **PPP** призначений для виконання тих же завдань, що й SLIP. Він працює як в асинхронному режимі з восьми бітами та контролем за парністю, так і в синхронному побітовому.

Складовою частиною PPP є протокол керування каналом. Він дає змогу формувати, реконфігурувати та тестувати послідовний канал. PPP виконує рекомендації мережевих протоколів керування (NCP), які, крім того, дають змогу зменшувати заголовки.

Структура кадру PPP зображено на рис. Д.13.4.1.

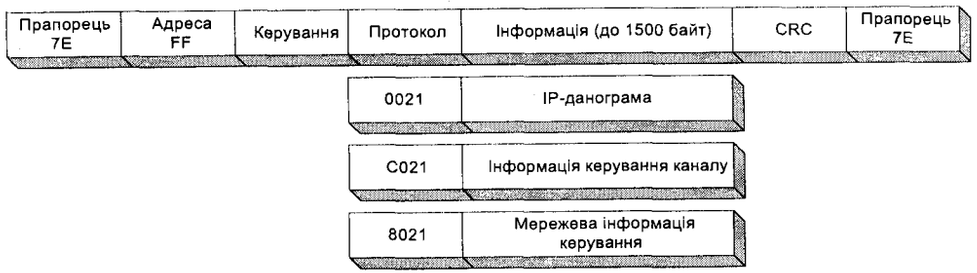


Рис. Д.13.4.1. Структура PPP-кадру.

На відміну від SLIP, PPP допускає мультипротокольність та динамічне визначення IP-адрес партнерів.

Д.13.5. Діагностика та повідомлення про збої (протокол ICMP)

Протокол **ICMP** (RFC-792, 1256) виконує діагностичні функції, повідомляє про збої та помилки. Перенесення ICMP-пакета відбувається за допомогою IP-пакета. ICMP посідає особливе місце в стеку протоколів TCP/IP. З одного боку, він використовує IP, і, отже, є на вищому рівні, однак з іншого, його система адресації та функції не відповідають нормам транспортного рівня, тому зачислити його до цього рівня не можна.

Головні функції ICMP такі:

- передавання відповіді на пакет або луна-відповіді;
- контроль часу наявності данограм у системі;
- переадресування пакета;

• надавання повідомлень про недосяжність адресата або некоректність параметрів;
• формування та пересилання часових позначок.

У деяких випадках формування ICMP-повідомлення заборонене (у відповідь на інше ICMP-повідомлення, у випадку циркулярного та групового передавання тощо) з метою запобігти лавинній генерації ICMP-пакетів.

Структура ICMP-пакета показана на рис. Д.13.5.1.

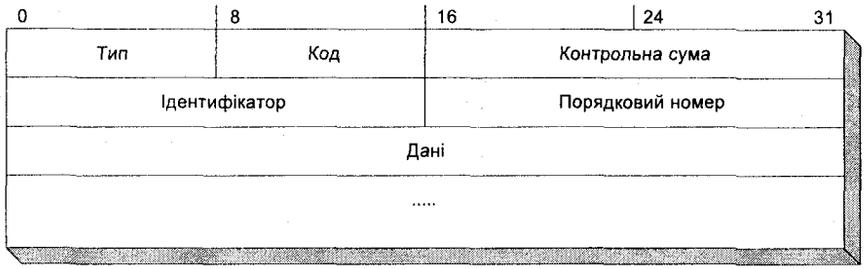


Рис. Д.13.5.1. Структура ICMP-пакета.

Поля *тип* та *код* визначають функцію ICMP-повідомлення. Приклади різних значень цих полів наведені в табл. Д.13.5.1.

Таблиця Д.13.5.1. Значення полів *тип* та *код* в ICMP-повідомленнях

Тип	Код	Опис повідомлення
0		Луна-відповідь ping
3		Адресат недосяжний
	0	Недосяжна мережа
	1	Недосяжна ЕОМ
	2	Недоступний протокол
	3	Недоступний порт
8	0	Луна-запит ping
13		Запит часової позначки
14		Часова позначка - відповідь
...	...	...

Поля *ідентифікатор* та *порядковий номер* потрібні для зіставлення запитів та відгуків. Розглянемо деякі приклади використання ICMP-пакета.

Приклад 1. Під час виконання процедури *Ping* луну-запит з часовою позначкою надсилають адресату. Якщо адресат активний, він приймає IP-пакет, міняє адреси відправника та одержувача місцями й відсилає пакет назад.

Приклад 2. Якщо маршрутизатор не в стані доставити даннограму за місцем призначення, він надсилає відправнику ICMP-повідомлення *адресат недоступний*.

Приклад 3. Якщо приймач не в стані прийняти потік вхідних повідомлень, він надсилає відправнику спеціальний запит (quench-запит) з вимогою зменшити інформаційний потік.

Приклад 4. Якщо маршрутизатор виявляє, що комп'ютер використовує неоптимальний маршрут, він надсилає ICMP-повідомлення з його корекцією. Крім того, маршрутизатори мережі періодично (через 500–600 с) циркулярно повідомляють про свої маршрути, що дає змогу іншим маршрутизаторам скоректувати таблиці.

Приклад 5. Однією з системних задач може бути задача синхронізації годинників. Для запиту часової позначки використовують ICMP-повідомлення *запит часової позначки*.

Д.13.6. Автоматизація конфігурування (протоколи RARP, BOOTP, DHCP)

Кожен комп'ютер у мережі TCP/IP щодо параметрів його конфігурування рівноправний з іншими комп'ютерами. Параметри конфігурування такі:

• IP-адреса;
• адреса сервера DNS;
• адреса шлюзу за замовчуванням.

Протоколи ARP, RARP

Протокол ARP (RFC-826) перетворює IP-адресу у канальну мережеву адресу. Протокол RARP (RFC-903) виконує зворотну дію – перетворює канальну адресу в IP-адресу. Гост, якому невідома його IP-адреса, надсилає у мережу циркулярний пакет-запит зі своєю MAC-адресою. Сервер RARP відповідає пакетом з IP-адресою.

Яким же чином сервер RARP відшукує відповідність між адресами? Кожен клієнт може визначити свою MAC-адресу за документацією адаптера або командою операційної системи. В системах Unix відповідність між MAC-адресами та іменами гостів задана у текстовому файлі /etc/ethers, наприклад:

```
2:80:8a:48:25:48   host1
4:6b:8a:48:25:49   host2
```

Для визначення IP-адреси використовують текстовий файл DNS hosts. Протокол RARP дає змогу одержати тільки IP-адресу.

Протокол самозавантаження BOOTP (Bootstrap protocol, RFC 951)

Первинне призначення протоколу BOOTP – автоматизоване завантаження комп'ютера. Проте він, крім того, дає змогу одержати і багато іншої інформації.

Клієнт, що завантажується, надсилає у мережу кадр запиту BOOTREQUEST, що містить MAC-адресу клієнта та передається за циркулярною адресою 255.255.255.255. Сервер відповідає пакетом BOOTREPLY. Під час роботи протоколу BOOTP задіяні порти UDP 67 (сервер) та UDP 68 (клієнт). Сервер передає дані про всі конфігураційні параметри, які йому відомі.

Сервер BOOTP запускають як демон на сервері Unix. Демон bootpd можна запустити або з файлу початкового завантаження rc.local, або опосередковано – через демон inetd. Він

обслуговує декілька портів одночасно. У текстовому файлі inetd.conf є список усіх демонів. Наприклад:

bootps dgram udp wait root /usr/etc/bootpd bootpd.

Демон bootpd можна запустити тоді, коли звернутися до нього.

Параметри, які можна одержати з сервера BOOTP: назва та місце розміщення завантажувального файлу, список серверів DNS, MAC-адреса, тип апаратного забезпечення, IP-адреса та ін. Інформацію клієнт одержує у вигляді текстового запису (файлу).

Протокол DHCP

Для додаткового сервісу щодо конфігурації адрес та реконфігурації мережі у великих мережах TCP/IP може діяти протокол **DHCP** (RFC-1541, 1534). DHCP – це удосконалений BOOTP. Він повністю сумісний з BOOTP, використовує ті ж порти (67, 68) та формат пакетів (BOOTREQUEST, BOOTREPLY). Однак у DHCP дещо розширений набір параметрів та є функція автоматичного поширення адрес.

У випадку використання DHCP адреси можуть бути у таких станах:

- закріплені за певними клієнтами та виділятися автоматизовано;
- виділятися автоматизовано з певної множини за випадковим законом;
- виділятися динамічно на визначений період часу.

Виділення адрес виконують спеціальні сервери DHCP. Розглянемо такий випадок. Нехай нову станцію приєднують до мережі, де функціонують сервери DHCP. Під час увімкнення ця станція (клієнт DHCP) надсилає циркулярне повідомлення *discover message – відшукати адресу.* Всі сервери DHCP відповідають на цей запит пропозицією унікальних мережевих адрес. Клієнт приймає пропозиції та переходить у стан вибору. У цей час сервери DHCP притримують запропоновані адреси. Клієнт обирає одну з них та повідомляє про це відповідний сервер. Сервери DHCP розблоковують невибрані адреси. Обраний сервер DHCP надсилає клієнту повідомлення підтвердження з додатковими конфігураційними параметрами.

Д.13.7. Протокол TCP

Протокол TCP, забезпечує передавання сегментів у вигляді байтових потоків з налагодженням сполучення. TCP використовують там, де потрібне гарантоване передавання повідомлення за призначенням. Для перевірки цілісності пакетів застосовують контрольні суми, для відстежування процесу передавання застосовують механізм вікон. TCP використовують такі прикладні процеси, як ftp, telnet та ін.

У системах, орієнтованих на сполучення, пара комбінацій IP-адрес та номерів портів однозначно задає канал зв'язку між двома комп'ютерами. Така комбінація називається **з'єднувачем** (Socket). Цей механізм уперше запроваджено в системі 4.3. BSD Unix. Його підтримує широкий набір команд.

Взаємодія TCP з протоколом верхнього рівня відбувається байт за байтом (потоково). На рівні TCP байти групуються у сегменти та передаються на рівень IP. TCP оптимізує розмір сегмента, що є змінним. Для контролю за часом, протягом якого повинно надійти підтвердження про одержання пакета, призначено таймер. Якщо за визначений час підтвердження не надійшло, передавання повторюється. Сегмент має максимальний час існування (Maximum Segment Lifetime (MSL)). З перевищенням цього часу він знищується.

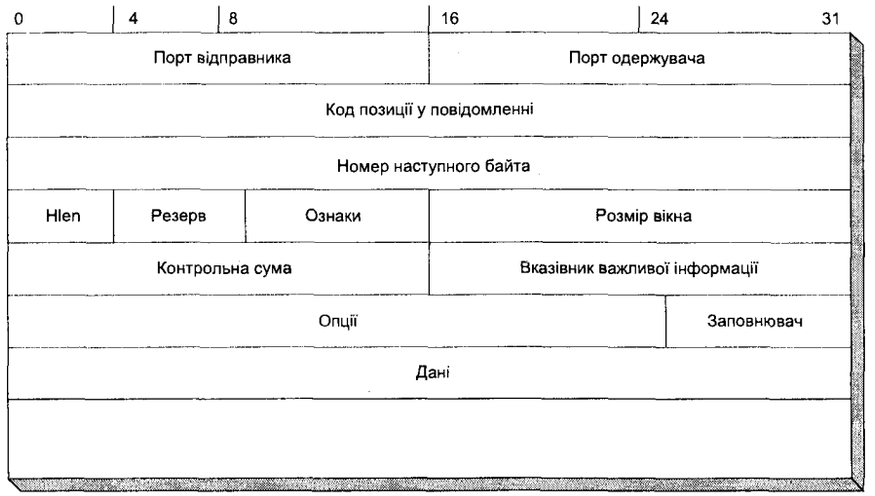


Рис. Д.13.7.1. Структура TCP-сегмента.

Першими полями сегмента є *порти відправника* та *одержувача* (рис. Д.13.7.1).

Код позиції в повідомленні визначає порядковий номер першого байта даних користувача.

Hlen – довжина заголовка сегмента.

Розмір вікна – кількість байтів, які готовий прийняти приймач.

Вказівник важливої інформації містить посилання на останній байт повідомлення, що потребує негайного реагування. Це поле має сенс тільки тоді, коли ознака *URG* – 1.

Поле *опцій* – це список полів змінної довжини. Кожна опція записується у форматі вид-довжина-зміст. Деякі опції – масштаб вікна, часова позначка.

Поле *даних* необов'язкове.

Значення деяких бітів з поля ознак: *URG* – ознака важливої інформації; *PSH* – якнайшвидше передати дані програмі застосування; *SYN* – ознака синхронізації номерів сегментів (використовують для налагодження сполучення); *FIN* – відправник закінчив відсилання пакетів.

Налагодження сполучення між клієнтом та сервером відбувається протягом таких трьох етапів:

- клієнт надсилає SYN-сегмент з зазначенням номера порту сервера, з яким потрібно налагодити сеанс зв'язку;

• сервер відповідає та надсилає свій SYN-сегмент, з ідентифікатором (ISN – Initial Sequence Number), який буде використано для нумерації сегментів під час передавання;

• клієнт надсилає підтвердження SYN-сегмента з номером ISN+1.

Кожне сполучення має свій ISN. Один з учасників обміну перебуває в пасивному режимі (passive open), інший – в активному (active open). Систему в протоколі TCP описують 11 станів. Частково стан системи можна проконтролювати командою netstat (рис. Д.13.7.2).

```
netstat -a -n
Proto  Local Address        Foreign Address     State
TCP    192.168.2.30:1025    192.168.2.1:139     ESTABLISHED   налагоджене сполучення
TCP    192.168.2.30:1038    198.168.2.22:139    TIME_WAIT     чекаємо роз'єднання
```

Рис. Д.13.7.2. Результат виконання команди *netstat*.

Для реалізації підтверджень у протоколі TCP використано метод змінних вікон.

Одним з важливих системних параметрів, які постійно вимірює TCP, є **RTT** (Round Trip Time) – час поширення сигналу до одержувача та назад. Цей параметр використовують для налагодження параметрів таймерів.

Сеанс зв'язку розпочинається надсиланням сегмента SYN, а закінчується сегментом FIN.

Д.13.8. Протокол UDP

Протокол **UDP** (RFC 768) – даграмний протокол транспортного рівня, що користується сервісом протоколу IP. Він не потребує підтвердження про одержання даграм. До заголовка IP-пакета додають поля порту відправника та порту одержувача, а також поля довжини повідомлення та контрольної суми (рис. Д.13.8.1).

Протокол UDP застосовують NFS, RPC, SNMP. Він характеризується невеликими накладними витратами. Незалежність окремих пакетів використовують multimedia.

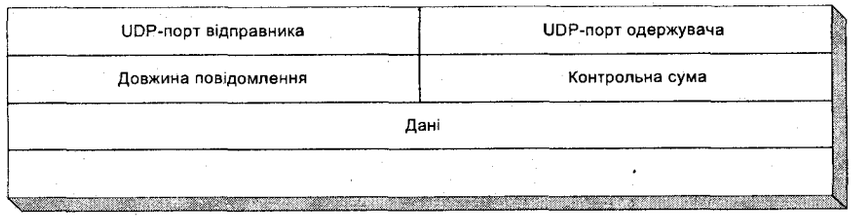


Рис. Д.13.8.1. Структура UDP-пакета.

Прикладні програми та модулі UDP взаємодіють через UDP-порти і пронумеровані від 0. Застосування, яке надає певні послуги (сервер), чекає повідомлень, надісланих у спеціально

виділений для цього порт (наприклад, SNMP завжди чекає повідомлення, адресованого порту 161. Тому на кожному комп'ютері може бути тільки один порт SNMP).

Дані, які передає застосування через UDP-модуль, потрапляють на місце призначення як єдине ціле. UDP не змінює переданих йому пакетів.

У системах Unix список стандартних номерів портів є у файлі /etc/services, наприклад:

```
Telnet    23/tcp      (застосування порт/протокол транспортного рівня)
netstat   15/tcp
smtp      25/tcp
echo      7/udp
time      37/udp
time      37/tcp
```

Порядок приймання IP-пакета. IP-модуль передає відповідний пакет UDP-модулю, якщо у заголовку пакета зазначено код протоколу UDP. UDP-модуль перевіряє контрольну суму в заголовку. Якщо вона не збігається, то пакет відкидається. В іншому випадку відбувається аналіз порту в пакеті. Повідомлення з пакета потрапляє в чергу до застосування, яке відповідає порту. Якщо черга переповнена, то UDP-модуль відкидає пакет.

Д. 13.9. Протоколи електронної пошти (SMTP, POP2, MIME, IMAP)

У мережах TCP/IP реалізовано декілька систем підтримки електронної пошти. Найбільш розповсюдженими є системи протоколів SMTP та UUCP (Unix to Unix Comminication Protocol).

У системах протоколів UUCP та X.400 зазначено всі проміжні гости, через які проходять повідомлення електронної пошти. Тому формат адреси, наприклад, такий:

serv1!serv2!serv3!user_dest

Повідомлення, яке не пройшло через якусь ланку ланцюжка, чекає на її доступність.

У системах протоколу SMTP реалізовано пряме доставляння повідомлення адресату. Адреса електронної пошти, наприклад, може мати вигляд

user1@dom1.dom2.com

Якщо ж комп'ютер адресата вимкнений, то повідомлення не буде доставлене.

Протокол SMTP працює з портом 25 та протоколом TCP. Головні команди цього протоколу такі:

Команда	Призначення
HELLO<гост-відправник>	Початок сеансу. Ідентифікація комп'ютера-відправника. Наприклад, HELLO dom1.dom2.com
MAIL FROM:<адреса відправника>	Передавання адреси відправника. Наприклад, MAIL FROM: user1@dom1.dom2.com

RCPT TO:<адреса одержувача>	Визначення адреси одержувача. Наприклад, RCPT TO: user2@dom1.dom2.com
DATA	Початок повідомлення
RSET	Переривання передавання повідомлення
VRFY<рядок>	Перевірка імені користувача. Можна, наприклад, одержати повну адресу користувача за його псевдонімом
EXPN<рядок>	Виведення змісту списку розсилання, що асоціюється з іменем певного користувача
HELP[<рядок>]	Надання допомоги
QUIT	Закінчення сеансу SMTP

Протоколи **POP** (Post Office Protocol) різних версій (POP2 – RFC-937, POP3 – RFC-1725) виконують аналогічні функції та використовують порти 109 та 110. Вони призначені для читання повідомлень з сервера для ПК. Ці протоколи працюють в *off-line* режимі, тобто головні операції з поштою виконує локальний комп'ютер після її надходження з поштового сервера.

Головні команди протоколу POP такі:

Команда	Призначення
HELLO користувач пароль	Початок сеансу та ідентифікація користувача
FOLD	Вибирання каталогу пошти
READ [n]	Читання повідомлень, починаючи з n-го
RETR	Читання повідомлення
ACKS	Підтвердження про збереження прочитаного повідомлення.
ACKD	Знищення повідомлення.
NACK	Виконати команду не можна.
QUIT	Закінчення сеансу

Під час сеансу POP2 користувач послідовно одержує повідомлення про кількість наявних листів, їхній обсяг. Він може прочитати лист, а потім його знищити або ж зберегти на сервері.

Протокол **IMAP** (RFC-1064, 1730) функціонально наближений до POP і дає змогу користувачу працювати з віддаленим сервером електронної пошти. На відміну від POP, IMAP може працювати в режимі *on-line*. Це означає, що головні операції над поштою виконуються безпосередньо на сервері. У цьому випадку забезпечується централізоване збереження поштової інформації та пов'язані з цим зручності оновлення, вірогідності, колективного використання, цілісності тощо.

Протокол **MIME** відомий як розширення протоколу SMTP. Протокол SMTP орієнтований на передавання текстової інформації в коді ASCII. MIME ж призначено для пересилання даних двійкового формату з використанням ASCII протоколів електронної пошти. Оскільки більшість Internet систем електронної пошти не придатні для передавання довільного двійкового символу, то MIME доводиться перетворювати байт у текстовий символ.

Нижче наведено зразки заголовків звичайного повідомлення та повідомлення MIME:

```
From: jpas@icm.lviv.ua
To: 72241.44@compuserve.com
Subject: See new version
....
```

```
From: jpas@icm.lviv.ua
To: 72241.44@compuserve.com
Subject: See new version
MIME-Version: 1.0.
Content-type: image/jpeg
Content-Transfer-Encoding: base64
.....
```

Отже, у заголовку повідомлення MIME є деякі поля, які описують тип та підтип даних, а також методи кодування-декодування.

Стандартні типи даних MIME наведені в табл. Д.13.9.1, а.методи кодування-декодування наведені в табл. Д.13.9.2.

Таблиця Д.13.9.1. Стандартні типи даних протоколу MIME

Тип	Підтип	Коментар
application	octet-stream postscript	Двійкові дані без перетворення Програма мовою postcript
audio	basic midi wav	Дані формату mu-law ISDN midi-формат wav-формат
image	gif jpeg	
message	rfc822 partial external-body	 Фрагмент більшого повідомлення Посилання на інше повідомлення
multipart	alternative digest mixed parallel	Багатокомпонентний об'єкт, що містить ту ж інформацію, але в різних форматах Об'єкт з повідомлень електронної пошти Об'єкт з незалежними частинами Об'єкт з залежними частинами, які опрацьовують паралельно
text	html plain richtext	Текст html- формату Звичайний текст Текст формату RTF
video	mpeg quicktime	Відео формату mpeg Відео формату quicktime

Приклад реалізації перетворення base64 показано на рис. Д.13.9.1.

Приклад перетворення quoted printable:

Copyright © 1996

Copyright =A9 1996

Таблиця Д.13.9.2. Методи кодування/декодування протоколу MIME

Значення	Коментар
7-bit	Без перетворення. Повідомлення містить 7-бітові символи
8-bit	Без перетворення. Повідомлення містить 8-бітові символи
base64	Кожна послідовність з трьох байтів перетворюється в чотири 6-бітові елементи - символи ASCII
binary	Без перетворень. Містить 8-бітові символи без символу переведення каретки
quoted-printable	Спеціальні символи замінені знаком 'дорівнює', після якого є двозначний 16-й код символу

Можна створювати власні підтипи даних, наприклад, image/x-myimageformat. Про нестандартний характер даних свідчить префікс 'x'. Нові типи та підтипи реєструють в IANA.

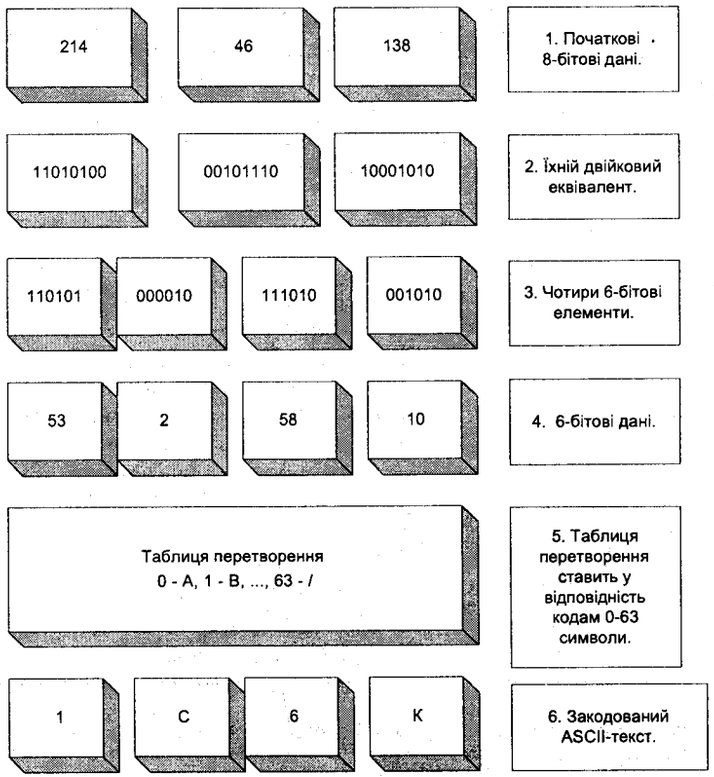


Рис. Д.13.9.1. Приклад реалізації перетворення base64.

Головні стандарти MIME такі:
RFC-1521 'MIME . Part One. Mechanisms for specifying and describing the format of Internet message bodies'.
RFC-1522 продовження.
RFC-1741 'MIME Content Type for Bin-Hex Encoded Files'.
RFC-1740 'MIME Encapsulation of Macintosh Files'.
RFC-1563 'The text/enriched MIME Content Type'.
RFC-1344 'Implications of MIME for Internet Mail Gateways'.

Д.13.10. Резервування ресурсів та підтримка ізохронних потоків (протоколи RSVP, RTP, RTCP)

Значна частина застосувань сучасних інформаційних мереж потребує передавання інформації у масштабі реального часу (ізохронні потоки). Вимоги до передавання таких потоків суттєво відрізняються від звичайних (наприклад, під час передавання файлів програм чи записів з баз даних). Головні відмінності такі:

• кадри з ізохронною інформацією повинні надходити до одержувача в такому ж темпі, з такими ж інтервалами, з якими їх створював відправник;

• допустима втрата деякої частини кадрів без суттєвого зменшення якості інформації в одержувача;

• над ізохронними потоками можна виконувати деякі додаткові операції (наприклад, злиття кількох потоків в один (мікшування) або передавання кількох варіантів одного і того ж потоку).

Звичайні, не ізохронні, потоки переважно не допускають втрати кадрів, однак інтервали та темп надходження кадрів може змінюватися у широких межах, бути непередбачуваним.

Найбільше для передавання ізохронної інформації придатні мережі ATM. Водночас переважною частиною сучасних локальних мереж є мережі Ethernet, які внаслідок особливостей свого методу доступу та через змінний розмір кадру не гарантують часу доставляння кадру. Використання швидкісних мереж Ethernet дещо вирішує проблему, особливо якщо є значний резерв у перепускній здатності. Значне зростання мережі Internet та протокольної архітектури TCP/IP потребую забезпечення ізохронного передавання на рівні пристроїв, що об'єднують локальні мережі (переважно маршрутизаторів), які часто є 'вузькими місцями'. Найчастіше пакети ізохронного потоку затримуються на деякий час (буферизуються), а потім надходять до одержувача у заданому темпі.

Транспортні протоколи TCP та UDP не підтримують ізохронного передавання. З цією метою створено нові протоколи RTP, RSVP, RTCP, IP Multicast та інші, що забезпечують ізохронність передавання на рівні маршрутизаторів.

Коротка характеристика протоколів:

• **RTP** (Real Time Reservation Protocol) забезпечує передавання даних з визначеними часовими параметрами;

• **RSVP** (Resource reservation Protocol) дає змогу замовити мережеві ресурси перед початком сеансу зв'язку (наприклад, з використанням протоколу RTP);

• **RTCP** (Real Time Transport Control Protocol) реалізує зворотний зв'язок з групою одержувачів інформації.

Протокол RTP

RTP є окремим протоколом (RFC-1889), який для передавання використовує протокол UDP. Для того, щоб пакети RTP надходили до адресата у тому ж темпі, в якому їх генерував відправник, кожен RTP-пакет має часову позначку (час його створення). Структура пакета показана на рис. Д.13.10.1.

Рис. Д.13.10.1. Структура RTP-пакета.

Зміст полів такий:

• поле версії;

• поле заповнювача (padding) визначає, чи є заповнювач до фіксованого числа 32-байтових слів;

• поле розширення заголовка визначає, чи використовується розширений формат заголовка;

• поле кількості відправників;

• поле маркера вказує на кінець логічного блоку даних (відеокадру або періоду мовчання);

• поле типу змістовної частини визначає тип та формат наведення інформації;

• пакети пронумеровані послідовно з метою виявлення їхніх втрат та визначення порядку пакетів з однаковою часовою позначкою;

• у часовій позначці записано час створення першого байта пакета;

• випадкове число, яке визначає унікальний номер джерела синхронізації.

Цікавою особливістю протоколу RTP є те, що він дає змогу передавати інформацію від багатьох джерел багатьом одержувачам. Злиття пакетів від багатьох джерел в одному RTP-пакеті називається *мікшуванням* (змішуванням). Фактично мікшування – це додавання ІКМ-

потоків (див. розділ 3). Прикладом операції мікшування є формування єдиного аудіопотоку накладанням звукових сигналів з кількох джерел. У спрощеному випадку мікшування зводиться до перетворення формату інформації з одного джерела. Така операція називається *транслюванням*. Прикладом транслювання є перетворення високоякісного формату відеосигналу у низькоякісний, але компактніший формат. Ідентифікатори окремих джерел записані у кінці RTP-пакета.

Передавання інформації протоколом RTP звичайно реалізується для групи станцій, визначених попередньо з використанням протоколу IGMP.

Протокол RTCP

Під час сеансу RTP необхідною є інформація зворотного зв'язку, оскільки дуже часто одержувачі не можуть приймати інформацію з визначеними якісними параметрами або ж у деяких ситуаціях виникає потреба динамічно зменшити швидкість чи інші параметри передавання. Для одержання такої зворотної інформації, а також для виконання деяких функцій керування і призначено протокол RTCP (RFC 1889). Він, як і RTP, використовує сервіс протоколу UDP і має свій номер порту. Головні функції RTCP такі:

• надання інформації від одержувачів даних. Протокол RTCP багатоадресний і всі одержувачі періодично розсилають усім учасникам сеансу інформацію про якість приймання інформації, нерівномірність потоку тощо. Це дає змогу діагностувати стан передавання і приймати рішення щодо зміни параметрів системи.

• одержання повнішої інформації про сеанс. Пакети протоколу RTP містять тільки ідентифікатор джерела синхронізації. Протокол RTCP доповнює протокол RTP функціями передавання текстового опису відправника, стану та структури потоків сеансу, видів та форматів даних, які передаються.

• масштабування сеансу. Без масштабування зі збільшенням кількості учасників сеансу кількість RTCP-пакетів могла б зайняти всю перепускну здатність каналів зв'язку і блокувати передавання первинної інформації. Тому важливою функцією протоколу RTCP є налагодження інтенсивності генерування пакетів залежно від кількості учасників сеансу. В цілому частка RTCP-пакетів не повинна перевищувати 5% від загального трафіку сеансу.

Протокол RSVP

Протокол RSVP дає змогу попередньо, перед початком сеансу, замовити потрібні ресурси на всіх проміжних маршрутизаторах. Він придатний як для одноадресного, так і для групового передавання.

Резервування ресурсів може відбуватися за участю як відправника, так і одержувачів інформації. У цьому принципи побудови протоколу RSVP відрізняються від принципів резервування, прийнятих, наприклад, у мережах ATM та Frame Relay. Відправники передають маршрутизаторам головні параметри інформаційного потоку (інтенсивність, рівномірність, формати

тощо). Однак основне рішення приймають на підставі 'замовлень', що надходять від одержувачів. Кожен з одержувачів, зважаючи на потреби та можливості, передає на маршрутизатори опис потоку, що складається зі *специфікації потоку та фільтра.* Специфікація потоку визначає якість обслуговування, а фільтр описує формат та ознаки пакетів, для яких потрібна така якість. Маршрутизатори приймають описи потоків від різних одержувачів та визначають узагальнені вимоги до потоків, які вони опрацьовують. У цьому випадку маршрутизатор може прийняти або відхилити запит на передавання. Пакети, що не відповідають вимогам фільтра, маршрутизатор передає у міру можливості.

Протокол RSVP використовує повідомлення типів *Resv* та *Path*. Повідомлення *Resv* власне резервують ресурси та переносять специфікації потоків і фільтрів. Маршрутизатори комбінують їх та передають від одержувачів інформації відправникам. Повідомлення *Path* мають на меті інформувати одержувачів про шлях до відправників (потрібний для передавання повідомлень *Resv*).

Порядок роботи протоколу такий:

- одержувач входить у групу одержувачів (з використанням протоколу IGMP);
- відправник надсилає повідомлення на адресу групи;
- одержувач приймає повідомлення *Path*, яке визначає відправника та шлях до нього;
- передаються повідомлення *Resv* для резервування ресурсів;
- відбувається сеанс передавання інформації.

Склад програмного агента RSVP містить модулі керування доступом (admission control) та адміністрування (policy control). Модуль керування доступом перевіряє наявність ресурсів для виконання запиту, а модуль адміністрування – наявність у застосування-автора запиту відповідних прав. Безпосередньо передаванням даних керують два модулі: *класифікатор пакетів (packet classifier)* та *диспетчер пакетів (packet scheduler)*. Класифікатор визначає належність пакета до певного класу обслуговування, а диспетчер опрацьовує черги пакетів, визначає пріоритетність передавання.

Багатоадресне та групове передавання

Для реалізації багатоадресного передавання гости повинні підтримувати протокол IGMP, а маршрутизатори – один з протоколів багатоадресної маршрутизації, а саме: **DVMRP** (Distance Vector Routing Protocol), **PIM** (Protocol Independent Multicast), **MOSPF** (Milticast Open Shortest Path First).

Д.13.11. Протокол IP. Використання поля опцій

Необов'язкове поле опцій в IP-пакеті має змінну довжину. Воно складається з записів однакового формату, кожен з яких відповідає певній опції (рис. Д.13.11.1).

Поле *код* описує тип опції. Байт коду поділено на три поля: *Ознака копії – клас опції – номер опції.* Додаткові поля уточнюють тип опції. Ознака копії приписує копіювати опцію у

інші фрагменти данограми. В іншому випадку вона є тільки у першій данограмі. Якщо клас опції дорівнює 0, то це пакет користувача або пакет мережевого керування; а якщо 2, то це пакет діагностики. У полі *номер опції* поняття класу деталізоване. Наприклад, номери 0–7 задають маршрут для трасування, 2–4 – часову позначку.

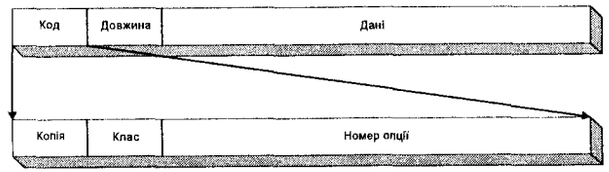


Рис. Д.13.11.1. Структура в полі *опції.*

Якщо задана опція запису маршруту, то кожен маршрутизатор на шляху пакета формує запис зі своєю IP-адресою (рис. Д.13.11.2).

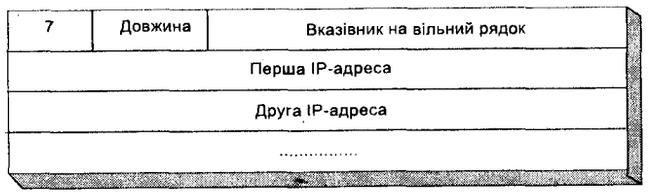


Рис. Д.13.11.2. Структура запису з IP-адресами.

Формат пакета для випадку, коли в полі опцій зазначено часові позначки, показано на рис. Д.13.11.3.

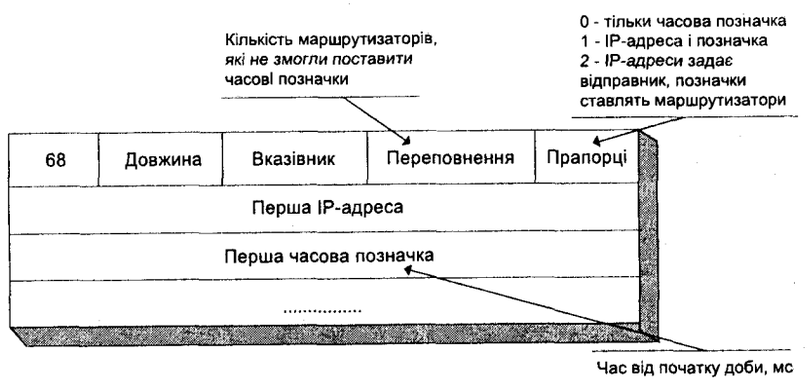


Рис. Д.13.11.3. Структура запису з IP-адресами та часовими позначками.

Д.13.12. Протоколи маршрутизації (загальна інформація)

Головний параметр маршрутизації IP-пакета – це його IP-адреса. Протокол IP поділяє всі ЕОМ на маршрутизатори (routers) та гости (hosts). Останні не розсилають маршрутних таблиць. Водночас на гості можуть бути запущені програми маршрутизації, тобто він може виконувати функції маршрутизатора.

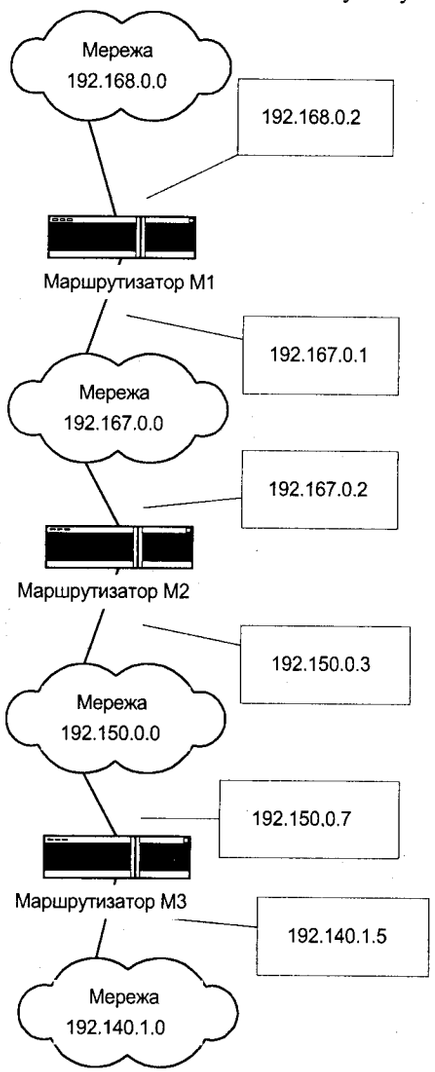


Рис. Д.13.12.1. Приклад маршрутизації.

Розглянемо приклад виконання маршрутизації (рис. Д.13.12.1).

Автономна система складається з чотирьох локальних мереж (у розумінні протокольного стека TCP/IP), сполучених трьома маршрутизаторами, кожен з яких є одночасно елементом кількох локальних мереж. Маршрутизатор має окрему IP-адресу в кожній мережі, по якій до нього звертаються гости цієї мережі. Маршрутна таблиця такої мережі для передавання пакета через М2 в найпростішому випадку могла б мати такий вигляд:

Мережа - адресат	Маршрут передавання
192.167.0.0	Пряме передавання
192.150.0.0	Пряме передавання
192.168.0.0	Через адресу 192.167.0.1
192.140.1.0	Через адресу 192.150.0.7

Елементом таблиці маршрутизації, як звичайно, є маршрут за замовчуванням (default). Якщо маршруту в таблицях не виявлено, то пакет надсилається за замовчуванням маршрутизатору, який має додаткову інформацію.

Алгоритм вибору маршруту:

1. IP-адреса читається з даграми.
2. У цій адресі відшукується адреса мережі призначення.
3. Якщо адреса відповідає локальній мережі, то пакет безпосередньо надходить до адресата.
4. Якщо адреса є в маршрутній таблиці, то пакет надсилається за цією адресою.
5. Якщо описано маршрут за замовчуванням, а адреси нема, то пакет надсилається за цим маршрутом.
6. Інакше подається повідомлення про помилку маршрутизації.

Якщо мережа має підмережі, то перед порівнянням адрес над IP-адресою призначення робиться побітове '&' з використанням маски.

Метрика маршруту – це його числова характеристика за критерієм: кількість проміжних маршрутизаторів, тривалість передавання, надійність тощо.

Найпоширеніші протоколи маршрутизації такі:

- **RIP** (Routing Information Protocol) RFC-1058, 1721, 27 – протокол внутрішньої маршрутизації для невеликих мереж. Розроблений фірмою Xerox. Простий, використовує одну метрику – кількість кроків. Його поступово витісняє протокол OSPF.
- **OSPF** (Open Shortest Pass First) RFC-1850, 1523, 1587, 1584 – протокол внутрішньої маршрутизації, складний, використовує кілька типів метрик.
- **EGP** (Exterior Gateway Protocol) RFC-904, 911, 1092, 1093 – протокол зовнішньої маршрутизації. Працює тільки з деревоподібними структурами мереж та повідомляє сусідам тільки про один можливий шлях. Його витісняє протокол BGP.
- **BGP** (Border Gateway Protocol) RFC-1267, 1771, 1655, 57 – протокол зовнішньої маршрутизації.
- **IGRP** (Interior Gateway Routing Protocol) – протокол внутрішньої маршрутизації, розроблений фірмою Cisco для великих неоднорідних мереж. Подібний до OSPF.

Д.13.13. Протокол внутрішньої маршрутизації RIP

Протокол RIP призначений для невеликих мереж. RIP-повідомлення інкапсулюються у даграми UDP. Використовується порт 520. Метрика маршрутизації – кількість кроків до мети. Наприклад, якщо між відправником та одержувачем три маршрутизатори, то значення метрики – 4. Така метрика не враховує різниць у перепускній здатності та завантаження окремих сегментів мережі.

Таблиця маршрутизації містить один запис про кожну машину, в якому зазначено таке: IP-адреса місця призначення, характеристика ціни маршруту (від 1 до 15), IP-адреса найближчого маршрутизатора, таймери маршруту.

Маршрут за замовчуванням має адресу 0.0.0.0. Кожен маршрут має таймери тайм-ауту та 'збирача сміття'. Таймер тайм-ауту скидається на нуль кожного разу, коли маршрут коректується або ініціалізується. Якщо з часу останньої корекції минуло 3 хв або одержано повідомлення, що відстань дорівнює 16, маршрут вважається закритим, однак запис про нього не стирається, поки не настане час 'збирати сміття'.

Структура повідомлення протоколу RIP зображено на рис. Д.13.13.1.

Поле *команда* має значення 1 для запиту і значення 2 – для відповіді. Значення поля *версія* становить 1 (для протоколу RIP2 – 2). Поле *набір протоколів* визначає протоколи, які використовуються у мережі (для Internet – 2). В одному повідомленні може бути інформація про 25 маршрутів і не більше.

Режими роботи RIP:

- ініціалізація – розсилання всім маршрутизаторам запитів, одержання від них таблиць;

• одержано запит – залежно від типу запиту надсилається вся таблиця або її частина;
• одержано відповідь – корекція таблиць.

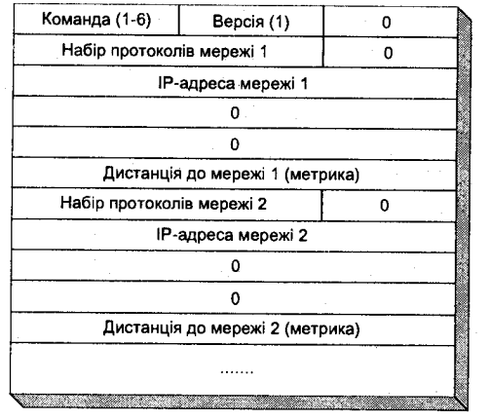


Рис. Д.13.13.1. Структура RIP-повідомлення.

Недоліки RIP:
• не працює з адресами підмереж, не може виділити підмережу;
• потрібно багато часу на відновлення після збою у маршрутизаторі;
• кількість кроків до мети – не найважливіша метрика, крім того, максимум у 15 кроків – це для сучасних мереж недостатньо.

У новій версії протоколу RIP2 (RFC-1721-24, 1993 р.) на додаток до циркулярного режиму підтримується групове передавання, можна працювати з масками підмереж. Структура RIP2-повідомлення зображено на рис. Д.13.13.2.

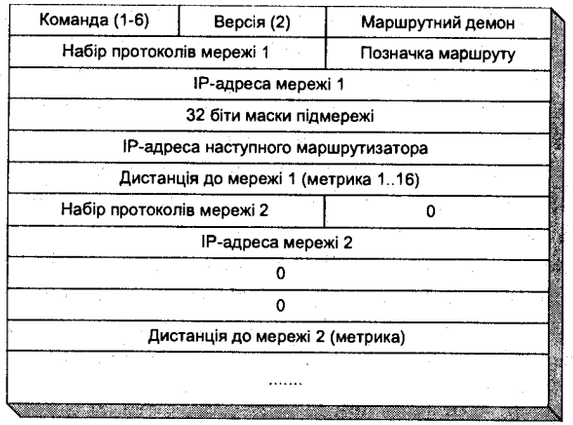


Рис. Д.13.13.2. Структура RIP2-повідомлення.

Поле *маршрутний демон* є ідентифікатором резидентної програми-маршрутизатора. У поле *позначка маршрутизації* записують коди автономних систем. Їх використовують для підтримки зовнішньої маршрутизації.

Д.13.14. Протокол маршрутизації OSPF

Протокол **OSPF** (Open Shortest Pass First) – це альтернатива протоколу RIP. Метрикою в ньому є якість обслуговування. Кожен маршрутизатор має повну інформацію про стан усіх інтерфейсів усіх маршрутизаторів автономної системи.

Автономна система може складатися з кількох зон. У цьому випадку внутрішні маршрутизатори зони можуть і не мати інформації про топологію іншої частини АС. Мережа звичайно має спеціальний призначений маршрутизатор, який є джерелом інформації для інших маршрутизаторів АС. Кожен маршрутизатор самостійно вирішує проблему оптимізації маршрутів, аналізуючи орієнтований граф мережі (алгоритми Дійкстри).

Якість обслуговування характеризується такими параметрами:
• перепускною здатністю каналу;
• затримкою в передаванні пакета;
• кількістю данограм, що є в черзі на передавання;
• завантаженням каналу;
• вимогами безпеки;
• кількістю кроків до мети.

Головними є затримка, перепускна здатність та надійність.

Для транспортних потреб OSPF використовує протокол IP напряму без проміжної інкапсуляції в UDP- або TCP-пакети. Маршрутизацію визначає IP-адреса та тип сервісу. Керування складними мережами з великою кількістю мостів та комутаторів у мережі протоколу OSPF спрощується.

Повідомлення OSPF мають заголовок, зображений на рис. Д.13.14.1.

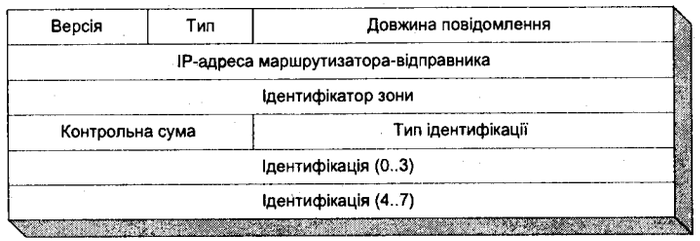


Рис. Д.13.14.1. Структура заголовка повідомлення OSPF.

Поле *Версія* визначає версію протоколу (2), поле *тип* – функцію повідомлення:
1 – повідомлення *hello*;

2 – опис бази даних (топологія мережі);
3 – запит про стан каналу;
4 – зміна стану каналу;
5 – підтвердження про одержання повідомлення щодо статусу каналу.

Поле *Ідентифікатор зони* містить 32-бітовий код зони. Всі OSPF-пакети асоціюються з певною зоною.

Одним з важливих є повідомлення типу *hello*. Цими пакетами обмінюються сусідні маршрутизатори. Структура такого пакета зображений на рис. Д.13.14.2.

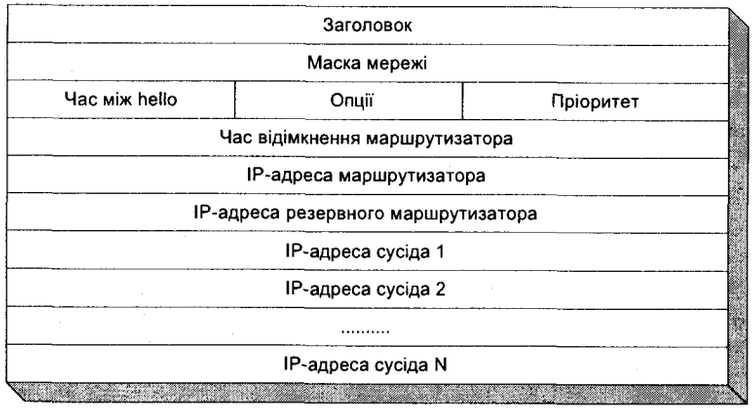


Рис. Д.13.14.2. Структура повідомлення *hello*.

Поле *Маска мережі* відповідає підмережі інтерфейсу, а поле *час між hello* задає час між повідомленнями цього типу.

Поле *опції* характеризує можливості маршрутизатора. У ньому є два біти керування – *E* та *T*. Біт *E* відповідає за зовнішню маршрутизацію. Якщо *E*=0, то маршрутизатор не буде взаємодіяти із зовнішніми автономними підсистемами. Біт *T* визначає сервісні можливості маршрутизатора. Якщо *T*=0, то це означає, що маршрутизатор підтримує тільки один різновид послуг. Такі маршрутизатори не використовують для транзитного трафіку.

Поле *Пріоритет* характеризує можливість використання маршрутизатора як резервного, поле *Час відімкнення маршрутизатора* – часовий інтервал, після закінчення якого 'німий' маршрутизатор буде вважатись відімкненим.

Поля *IP-адреса сусіда* є списком адрес сусідніх маршрутизаторів, від яких останнім часом були одержані повідомлення *hello*.

Другий тип пакета відповідає інформації про топологію мережі з бази даних OSPF, яка є на кожному маршрутизаторі. Маршрутизатори обмінюються повідомленнями цього типу з метою ініціалізації та актуалізації інформації в своїх базах даних щодо стану топології мережі. Обмін відбувається в режимі 'клієнт–сервер'. Клієнт підтверджує одержання кожного повідомлення. Структура цього пакета зображений на рис. Д.13.14.3.

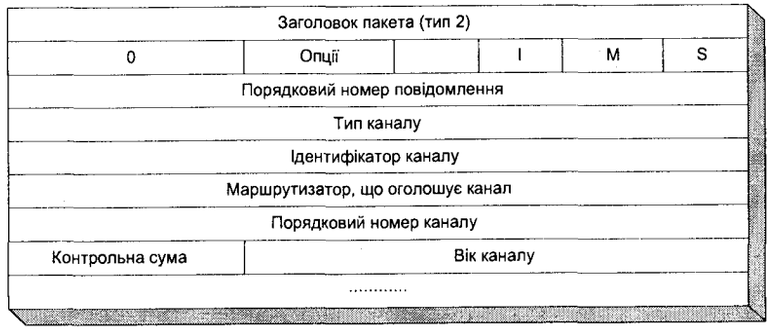


Рис. Д.13.14.3. Структура пакета про опис бази даних.

Розмір бази даних може бути значним і тому передбачена можливість її пересилання частинами. Для цього використовують біти *I* та *M*. Біт *I* дорівнює 1 в стартовому повідомленні, а біт *M* – у повідомленнях продовження. Біт *S* визначає, хто надіслав повідомлення (0 – клієнт, 1– сервер).

Порядковий номер повідомлення призначений для контролю пропущених блоків. Поля, починаючи з поля *Тип каналу*, повторюються для кожного опису каналу. Значення поля *Тип каналу* такі: 1 – опис стану інтерфейсів маршрутизатора, а також каналів, що виходять з нього; 2 – опис мережевих каналів; 3 – канали до граничних маршрутизаторів зон; 4 – канали до граничних маршрутизаторів автономної системи; 5 – зовнішні зв'язки автономної системи.

Поле *Ідентифікатор каналу* визначає характер каналу. Ним може бути IP-адреса маршрутизатора або мережі. Поле *Порядковий номер каналу* дає змогу маршрутизатору контролювати порядок надходження повідомлень та їхню втрату. Поле *Вік каналу* задає час з моменту налагодження зв'язку в каналі.

Пакет третього типу – *Запит про стан каналу* – надсилають з метою одержати інформацію про стан каналу. Її надсилає сусід, що одержав запит. Структура запиту зображений на рис. Д.13.14.4.

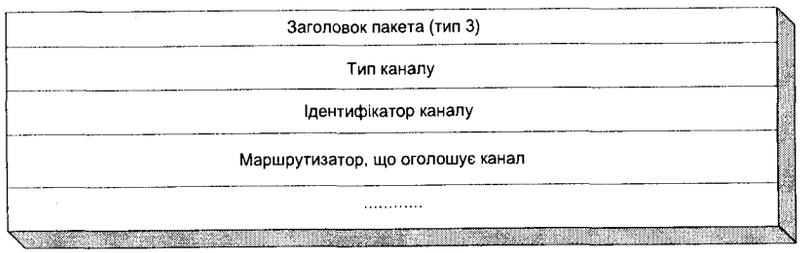


Рис. Д.13.14.4. Структура *Запиту про стан каналу*.

Останні три поля повторюються залежно від кількості каналів, інформація про які потрібна. Якщо стан каналів, безпосередньо сполучених з маршрутизатором, змінився, то надсилаються циркулярні або групові повідомлення. Можливі причини розсилання повідомлень

такі: вік маршруту досяг граничного значення, змінився стан інтерфейсу, відбулися зміни в маршрутизаторі тощо. Структура пакета показаний на рис. Д.13.14.5.

Заголовок пакета (4)
Кількість повідомлень про стан каналу
Повідомлення про стан каналу 1
.....
Повідомлення про стан каналу N

Рис. Д.13.14.5. Структура повідомлення про зміну стану каналу.

Повідомлення про стан каналу має свою структуру. Його структура може залежати від типу каналу (рис. Д.13.14.6).

Заголовок					
Вік оголошення каналу				Опції	1
Ідентифікатор оголошення каналу					
Маршрутизатор, що оголошує канал					
Номер запису про канал					
Контрольна сума				Довжина	
0	V	E	B	0	Кількість каналів
Ідентифікатор каналу					
Опис каналу					
Тип			Кількість TOS		Метрика TOS
Код TOS			0		Метрика
.....					
Код TOS			0		Метрика
Ідентифікатор каналу					
Опис каналу					
.....					

Рис. Д.13.14.6. Структура повідомлення про стан каналу.

Коди TOS (Type of Sevice) такі:

0	Звичайний сервіс
2	Мінімізація вартості
4	Максимальна надійність
8	Максимальна перепускна здатність
16	Мінімальна затримка

Біт *E*=1, якщо маршрутизатор є граничним для автономної системи, біт *B*=1, якщо маршрутизатор є граничним для зони.

Д.13.15. Зовнішня маршрутизація та маршрутна політика

Автономні системи проводять кожна власну маршрутну політику, користуються одним протоколом внутрішньої маршрутизації та сполучені з іншими автономними системами за допомогою граничних маршрутизаторів, через які проходить весь транзитний трафік (рис. Д.13.15.1).

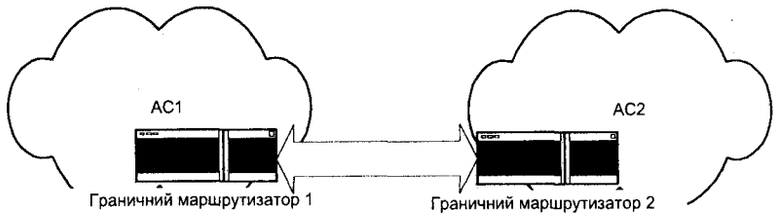
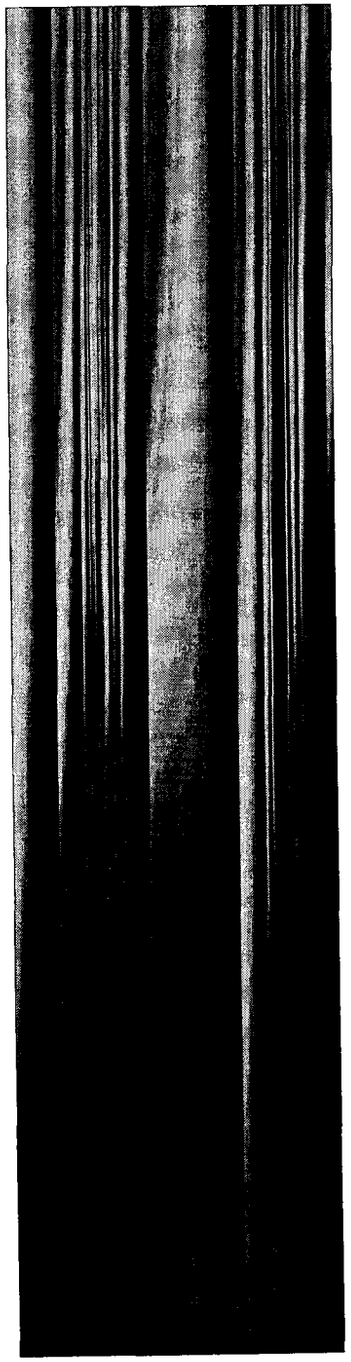


Рис. Д.13.15.1. Зовнішня маршрутизація.

Одним із протоколів зовнішньої маршрутизації є **BGP** (Border Gateway Protocol) (RFC-1267, 1655, 1771-74). На відміну від маршрутизаторів, що є всередині автономної системи, граничні маршрутизатори можуть сполучувати АС з різними протоколами маршрутизації. Кожен граничний маршрутизатор формує свої власні маршрутні таблиці і повідомляє сусідні граничні маршрутизатори про зміни у них. Маршрутні таблиці зберігаються у спеціальній базі даних маршрутів **RIB** (Routing Information Base).

На відміну від внутрішніх маршрутизаторів граничні маршрутизатори не зобов'язані передавати всю інформацію на інші маршрутизатори. (Один граничний маршрутизатор не зобов'язаний надсилати, а інший – приймати). Протокол визначає тільки формат інформації, порядок обміну.

Тому важливою є політика маршрутизації. Її задає адміністратор, який визначає параметри обміну маршрутною інформацією, часові параметри, канали, яким треба надавати перевагу та інше, враховуючи не тільки технічні, але й юридичні, економічні та інші обставини.



Частина 2

МЕРЕЖЕВІ ТЕХНОЛОГІЇ

ВІДДАЛЕНИЙ ДОСТУП ТА ОБ'ЄДНАННЯ ЛОКАЛЬНИХ МЕРЕЖ

Проблема сполучення локальних мереж. Метод віддаленого клієнта. Дистанційне керування. Сервери доступу та модемні сервери. Сервер асинхронного зв'язку. Інтелектуальні засоби сполучення ЛМ. Повторювачі. Призначення та головні функції мосту. Комутатори. Алгоритм залишкового дерева. Маршрутизатори, їхнє функціональне призначення. Принципи роботи маршрутизатора. Шлюзи. Порівняння сфер застосування та принципів дії мостів і маршрутизаторів.

Після створення та налагодження роботи локальної мережі постає проблема віддаленого доступу до неї та зв'язку користувачів цієї мережі з даними та користувачами з інших локальних та глобальних мереж. Процес налагодження такого зв'язку, як звичайно, відбувається поступово та потребує значних коштів і часу. На кожному етапі розвитку інформаційної системи повинен бути досягнутий максимум співвідношення *ефективність/затрачені кошти*. У цьому розділі ми розглянемо головні засоби й можливості віддаленого доступу та сполучення локальних мереж.

Для сполучення з локальною мережею можна застосувати такі методи:

- метод віддаленого клієнта;
- дистанційне керування;
- модемний зв'язок;
- інтелектуальні засоби зв'язку.

14.1. Метод віддаленого клієнта

Суть методу віддаленого клієнта полягає в такому. Віддалений комп'ютер приєднують через модем. Програма переспрямування (redirector, див. розділ 33) в цьому комп'ютері розглядає модем як повільний адаптер мережі і спрямовує на нього весь інформаційний потік. Це уповільнює роботу комп'ютера (унаслідок малої швидкості передавання даних через модем і великих обсягів інформації, що передається). Однак такий підхід широко використовують на практиці (особливо для приєднання мобільних користувачів) (див. розділ 13. Протоколи SLIP та PPP).

14.2. Дистанційне керування

У цьому випадку віддалений комп'ютер також приєднують через модем. Однак через модем передається не вся інформація, а тільки керування (коди натиснутих клавіш, екранні

зображення тощо), а опрацьовуються дані комп'ютером локальної мережі. Клавіатура та екран віддаленого комп'ютера працюють паралельно з клавіатурою та екраном комп'ютера у мережі. Отже, працівник може, залишивши свій комп'ютер на робочому місці увімкненим, продовжити роботу на ньому вдома, скориставшись домашнім комп'ютером, модемом та програмним забезпеченням віддаленого контролю. Віддалений контроль використовують широко, проте для цього потрібно задіяти комп'ютери в мережі. Зовнішні користувачі, які не мають власних комп'ютерів у мережі, працювати з дистанційним керуванням не можуть. Крім того, зі збільшенням бажаючих працювати у мережі з віддалених комп'ютерів такий спосіб стає неефективним. Тому актуальним є перехід до серверів доступу, модем-серверів та серверів асинхронного зв'язку.

14.3. Модемний зв'язок

Сервер доступу (access server) – це спеціалізований пристрій, приєднаний до ЛМ, що має свій власний процесор(и) і виконує запити щодо обчислення, які надходять з модемів. Як звичайно, сервер доступу приймає виклики одночасно з кількох модемів та обслуговує їх на своїх процесорах.

Сьогодні є три архітектури серверів доступу.

- Багатопроцесорна система. Кожен модем приєднаний до окремої плати з процесором та пам'яттю. Всі плати через один адаптер мережі приєднані до мережі.
- Багатопроцесорна система. Кожен модем приєднаний до окремої плати з процесором та пам'яттю. Кожна плата приєднана до окремого адаптера.
- Однопроцесорна система або персональний комп'ютер, який працює в режимі розподілу часу для опрацювання окремих викликів та приєднаний до мережі через адаптер. Така система дешевша, ніж багатопроцесорні, але ненадійна. Зависання одного процесу може призвести до зависання інших.

Модем-сервери, на відміну від серверів доступу, використовують для обслуговування викликів, що виходять з мережі. Їхня ефективність зумовлена потребою економного використання телефонних ліній, оскільки оренда окремої лінії коштує дорого. Як звичайно, кілька модемів та один модем-сервер обслуговують зовнішні виходи користувачів великої ЛМ.

Сервер асинхронного зв'язку – це пристрій, який поєднує функції сервера доступу та модем-сервера, тобто опрацьовує вхідні та вихідні виклики.

14.4. Інтелектуальні засоби сполучення локальних мереж

Головні інтелектуальні засоби сполучення ЛМ такі:

- повторювачі;
- мости;
- маршрутизатори;
- шлюзи.

Повторювачі (repeaters) – це найдешевші засоби зв'язку ЛМ, які не можна в прямому значенні слова вважати 'інтелектуальними'. Вони перепускають увесь потік між ЛМ, збільшують допустиму довжину кабелю та поновлюють амплітуду і форму сигналів. Повторювачі працюють на фізичному рівні протоколу. Їх часто розміщують між сегментами однієї ЛМ (рис. 14.1).

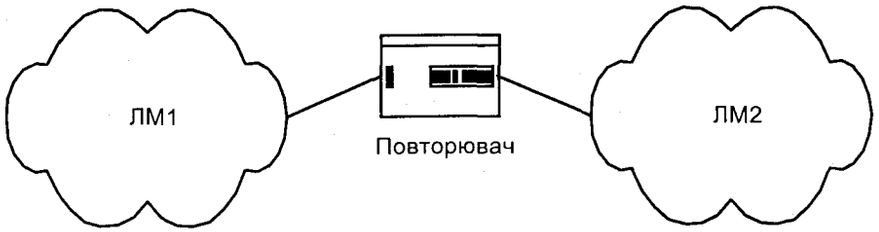


Рис. 14.1. Використання повторювачів у ЛМ.

Функціонально близькими до повторювачів є **концентратори** (hubs). Недоліком шинних кабельних мереж була ненадійність, труднощі, пов'язані з діагностуванням. З появою зіркової топології, у якій концентратор розміщений у центрі зірки, вся комутована частина зосереджена в одному місці. Це спрощує процес діагностування та приєднання нових користувачів.

Концентратори працюють як повторювачі. Для них залишається чинним обмеження на кількість повторювачів у мережі (не більше чотирьох для мереж 10Base-X). У разі використання концентраторів у мережі виникає спільне середовище передавання та єдиний домен колізій. Багатопортові концентратори ретранслюють інформаційний потік на всі порти.

У 'звичайних' концентраторах станції чітко закріплені за портом. Якщо ж виникає потреба змінити порт, то для цього потрібно виконати фізичну перекомутацію. Однак є концентратори, які можуть перемикати порти логічним, програмним шляхом (configuration switching hubs). Концентратори працюють на фізичному рівні протоколу, не фільтрують потік, не зменшують завантаження мережі і не знімають обмежень на довжину мережі з повторювачами.

Мости (bridges) – це апаратно-програмні блоки, які дають змогу сполучати ЛМ з різними середовищами передавання та протоколами (наприклад, мережі Ethernet, Arcnet, Token Ring, X.25). Вони працюють на канальному рівні й аналізують адреси в кадрах. Головна функція мосту – фільтрування кадрів між приєднаними сегментами і, як наслідок, зменшення їх завантаженості. Міст аналізує весь потік в усіх приєднаних сегментах, він прозорий для протоколів мережевого рівня та вище. Це пристрій повинен вирішувати такі можливі проблеми: незбіжність форматів кадрів, різниця в перепускній здатності та завантаженості, максимальному розмірі кадру сполучуваних сегментів. Правила функціонування мостів регламентує стандарт IEEE-801.d.

Розрізняють внутрішні та зовнішні мости. Внутрішній міст – це встановлені в одному сервері кілька адаптерних плат різних ЛМ (до чотирьох). Така конструкція дає змогу сполучити кілька ЛМ з різними або однаковими середовищами та протоколами. Для такого мосту потрібне спеціальне програмне забезпечення.

Зовнішній міст – це міст, реалізований у спеціальній машині. Він може бути **призначеним** або **непризначеним** (dedicated та non dedicated). Непризначений міст, крім функцій мосту, виконує ще й деякі прикладні функції. Збої в роботі прикладного процесу можуть перешкодити роботі непризначеного мосту і впливають на транзакції. Призначений міст виконує тільки функції мосту і ліпше захищений від збою.

Функціонально близьким до мосту є **комутатор** (switch). Компанія IDC визначає його так: 'комутатор – це пристрій, конструктивно виконаний у вигляді мережевого концентратора, що працює як високошвидкісний багатопортовий міст; вбудований механізм комутації дає змогу виконувати сегментування локальної мережі та виділяти смугу перепускання кінцевим станціям мережі' [5]. Детальніше технологія комутації локальних мереж описана в розділі 19.

Відомо два підходи до створення мостів. Перший з них, найпоширеніший, реалізований у мережах Ethernet, а другий – в мережах Token Ring.

Розробники концепції мосту **Transparent Bridging** ставили за мету створення повністю прозорого мосту. На їхню думку, міст повинен об'єднувати мережі без додаткового налагодження, достатньо тільки приєднати кабелі (рис. 14.2).

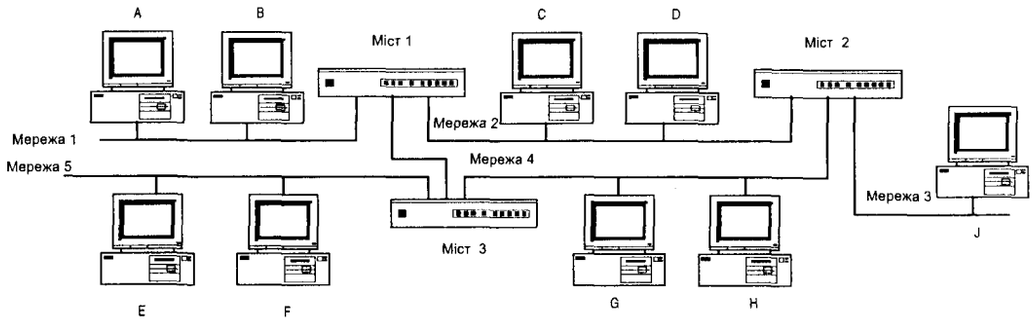


Рис. 14.2. Мережа з алгоритмом прозорого мосту.

Прозорий міст приймає всі кадри. Висновок про спрямування кадру у конкретний вихідний порт він робить на підставі таблиці адрес, яка ставить у відповідність усі відомі мосту адреси призначення лініям (портам), куди треба спрямувати кадр. Під час першого вмикання мосту всі його таблиці порожні. До відшукання співвідношень діє алгоритм радіального розсилання: кадр, для якого не визначено вихідний порт, спрямовується в усі порти, крім порту з якого він надійшов. Прозорі мости визначають місцеперебування адресатів з використанням алгоритму зворотного навчання (backward learning): приймаючи всі кадри, міст аналізує адресу відправника та визначає, через який порт цей відправник доступний.

Топологія мережі може змінюватися внаслідок переміщення мостів та робочих станцій. Для врахування такої динаміки кожен адресний запис таблиць мосту містить час одержання кадру. У випадку одержання кадру з уже відомим відправником час у записі поновлюється. Періодично міст переглядає всю таблицю і вилучає записи, вік яких перевищує визначений

час (кілька хвилин). У результаті, якщо комп'ютер перевести в іншу локальну мережу, то вже через кілька хвилин він зможе нормально працювати. Все відбувається без втручання людини. Водночас якщо станція не надсилає дані протягом визначеного часу, то весь призначений їй трафік буде пересилатись на всі сусідні мережі.

Загальні правила спрямування кадру мостом такі:

• якщо відправник та одержувач є в одній мережі, то кадр відкидається;

• якщо відправник та одержувач є в різних мережах (по різні боки від мосту), то кадр спрямовується у вихідний порт згідно з адресними таблицями;

• якщо визначити вихідний порт не вдалося, то кадр розсилається на всі порти, крім порту, з якого він надійшов.

З метою запобігти зациклюванню кадрів у складних мережах з багатьма мостами використовують алгоритм залишкового дерева, тобто у мережі формують деревоподібну структуру, яка об'єднує всі станції. Канали, які не увійшли в дерево, є резервними й інформації не передають. Якщо канал або комутатор вийшли з ладу, то дерево перебудовується, використовуючи резервні канали (див. Д.14.1).

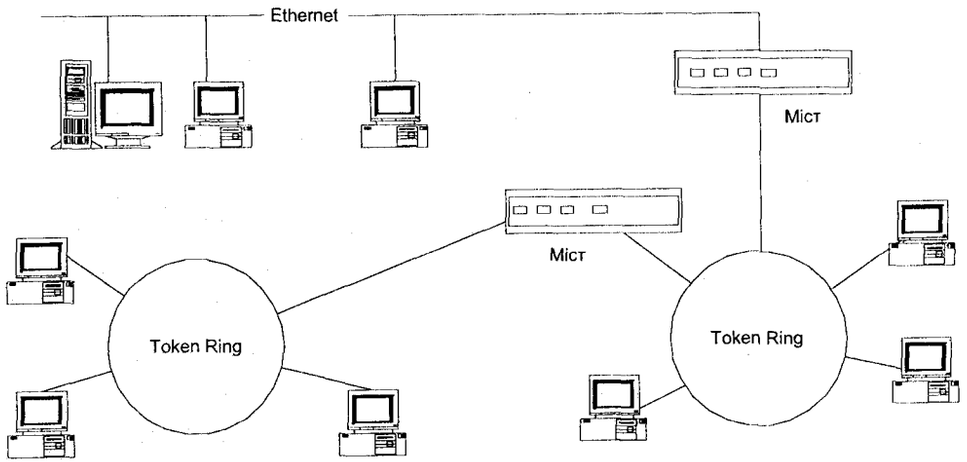


Рис. 14.3. Мережа з алгоритмом мосту з запитом джерела.

Альтернативою для прозорих мостів, які використовують у мережах Ethernet, є мости з визначенням шляху за запитом джерела (Source Routing), що їх застосовують у мережах Token Ring (TR) (рис. 14.3). Згідно з цим алгоритмом головні функції маршрутизації виконують не мости, а станції. Відправник кадру повинен знати, що одержувач є в іншій мережі (у цьому випадку старший біт адреси дорівнює 1). Крім того, в заголовку кадру записано весь шлях, що його повинен пройти кадр. Кожна мережа має унікальний 12-бітовий, а міст – 4-бітовий номер, за якими їх можна однозначно ідентифікувати в межах конкретної мережі. Це означає, що номери мостів, сполучених з конкретним кільцем TR, унікальні. Шлях є послідовністю номерів: міст, мережа, міст, мережа, … .

Міст TR опрацьовує тільки ті кадри, в яких старший біт адреси дорівнює 1. Функція мосту полягає в опрацюванні послідовності номерів шляху. Якщо станція-відправник не знає шляху до одержувача, вона надсилає *розшуковий кадр (discovery frame)*. Цей кадр передають усі мости у мережі, і в результаті він потрапляє до всіх станцій. Відповідь також розсилається циркулярно, кожен міст на шляху кадру записує в нього інформацію про час руху кадру та про себе. Унаслідок цього, станція, що передала розшуковий кадр, має змогу проаналізувати одержану інформацію та вибрати оптимальний шлях, який кешується у відправника. Суттєвим недоліком алгоритму мосту TR є експоненційне зростання завантаженості мережі розшуковими кадрами. Наприклад, якщо в мережі є N мереж і між кожною парою мереж по три мости, то загальна кількість розшукових кадрів 3^{N-1}.

Прозорі мости невидимі для робочих станцій, не потребують їхнього додаткового завантаження. У мережі TR станції повинні мати інформацію про наявність мостів та активно співпрацювати з ними, введення нового мосту потребує переконфігурації програмного забезпечення станцій. Зі зміною топології мережі прозорі мости переконфігуровуються автоматично, а з мостами TR це треба робити вручну. У цьому випадку можливі помилки (наприклад, дублювання номерів) виявити важко. Однак теоретичною перевагою мостів TR є змога використовувати оптимальний шлях пересилання кадрів, тоді як у мережах Ethernet цей шлях обмежено деревом. Різними є і реагування на аварії. У мережі з прозорими мостами про вихід компоненти з ладу мости дізнаються швидко і відбувається переконфігурування залишкового дерева. Якщо ж вийде з ладу один з мостів TR, то відправник інформації вчасно не одержить підтвердження. Він ще декілька разів спробує передати інформацію і тільки після цього відішле розшуковий кадр. Таку ж процедуру виконають інші станції, що передавали інформацію через несправний міст. Недоліком прозорих мостів є циркулярне передавання кадрів у разі, коли нема зворотних передавань від одержувача, а недоліком мостів TR – експоненційне збільшення кількості розшукових кадрів у складних мережах. Крім того, навряд чи доцільно додатково завантажувати станцію функціями мосту. Якщо ж урахувати велику кількість станцій та сумарні задіяні ресурси, то вказівник задіяних ресурсів виявиться значно більшим, ніж у випадку реалізації тих же функцій у кількох мостах.

Підкомітет IEEE-801.1d не визначив єдиного стандарту для мостів між локальними мережами, тому прийнято два несумісні стандарти для мостів. Згодом обидва методи організації мостів об'єднали в єдиному стандарті Source Routing Transparent. Такий міст може одночасно працювати і як Source Route, і як Transparent.

З наведеного вище можна зробити такі висновки:

• міст дає змогу не обмежувати кількість сегментів у ЛМ та загальну тривалість поширення сигналу;

• за допомогою мосту можна сполучити декілька мереж різного типу або з різними середовищами передавання;

• міст, як комутатор (див. розділ 19), дає змогу реалізувати технологію комутації локальних мереж з усіма її перевагами;

• міст надає адміністратору додаткові засоби для фільтрування потоку між групами станцій, що підвищує загальну безпеку системи.

Маршрутизатори (routers) – це апаратно-програмні пристрої, які дають змогу сполучати різні ЛМ та виконують, як і мости, функцію маршрутизації. Однак, на відміну від мостів, маршрутизація в них виконується на мережевому рівні. Кожен порт маршрутизатора має свою канальну та мережеву адреси, як і робоча станція. Станція, яка хоче передати пакет у зовнішню ЛМ, формує кадр з адресою порту маршрутизатора і надсилає його. Тому маршрутизатор опрацьовує не весь інформаційний потік у мережі, а тільки кадри, що адресовані безпосередньо йому. Він відкидає адресну інформацію канального рівня і далі працює з пакетом мережевого рівня, аналізуючи мережеву адресу. На підставі мережевої адреси і внутрішніх таблиць маршрутизатора пакет буде спрямовано через інший порт до наступного вузла мережі за оптимальним маршрутом. У цьому випадку формується кадр нової мережі.

Маршрутизатори бувають статичними та динамічними. Статичні маршрутизатори мають постійні таблиці маршрутизації. У динамічних же висновок про шлях спрямування приймається на підставі інформації про відносну ефективність та надійність окремих шляхів. Маршрутизатори ефективніше використовують канали зв'язку, проте складніші та дорожчі порівняно з мостами. Вони, як звичайно, спричинюють більшу затримку під час передавання даних, ніж мости та комутатори. Головні принципи організації та роботи сучасного маршрутизатора розглянуті в Д.14.2. Робота маршрутизаторів у випадку реалізації протоколів мережі internet описана в розділі 13.

Зважаючи на порівняно високу вартість маршрутизаторів та комутаторів, велику затримку, яку спричинюють маршрутизатори, функції маршрутизації та комутації часто виконує один пристрій (див. Д.14.3).

Шлюз (gateway) – це машина або порт колективного доступу, який об'єднує кілька мереж, або його використовують для приєднання мережі до головної ЕОМ (mainframe). У цьому випадку, як звичайно, перетворюються формати даних. Тому шлюз працює з протоколами верхніх рівнів (сеансовий, відображення, прикладний). Реалізація шлюзів значно дорожча, проте інтелектуальні можливості їхні значно більші порівняно з мостами і маршрутизаторами.

14.5. Сфери застосування мостів та маршрутизаторів

Відомо, що звичайна робоча станція в локальній мережі на канальному рівні виконує функцію селекції інформації – вибирає з загального потоку кадрів ті, що адресовані їй. У цьому випадку вона порівнює MAC-адресу призначення в кадрі зі своєю адресою.

Міст також виконує селекцію інформації. Однак, на відміну від станції, він порівнює адресу призначення з усіма адресами станцій у своїх таблицях. Для прийняття адекватного рішення у цих таблицях повинні бути адреси всіх станцій локальної мережі. Зрозуміло, що з ускладненням мережі збільшується й обсяг таблиць. Комутатор, крім того, повинен пам'ятати таблиці щодо всіх своїх портів (інтерфейсів). Прозорий міст, аналізуючи адреси, одночасно коректує свої таблиці. У випадку значного збільшення мережі, якщо мости не встигають аналізувати таблиці або виникло переповнення, вони переходять на радіальне передавання кадрів. Отже, мости та комутатори працюють в умовах великого завантаження.

Крім того, мости мають такі відмінності від маршрутизаторів:

- не блокують циркулярні передавання. Якщо трапиться збій, то це може призвести до значного перевантаження мережі;
- працюють з топологією залишкового дерева. У цьому випадку не використовуються резервні шляхи та комутатори;
- не перетворюють протокольну інформацію мережевого рівня. З погляду цього рівня мережа з мостами – це одна мережа.

Маршрутизатори працюють на мережевому рівні. Це означає, що на канальному рівні у порті маршрутизатора відбувається селекція інформації. На мережевий рівень маршрутизатора надходить не весь потік інформації, а тільки безпосередньо адресований йому. Отже, маршрутизатор порівняно з мостом значно менше завантажений. Маршрутизатор також не зобов'язаний зберігати інформацію про топологію всієї мережі, а тільки автономної системи (див. розділ 13). У випадку невизначеної адреси пакет може буги спрямований до певного граничного маршрутизатора. За рахунок меншого навантаження маршрутизатор може виконувати інтелектуальніші функції, пропонувати резервні канали та ін. Крім того, на відміну від мостів, маршрутизатори блокують циркулярні пакети, реалізують передавання пакетів кількома шляхами.

Отже, мости доцільно застосовувати у невеликих та середніх мережах. Зі збільшенням мереж доводиться використовувати маршрутизатори.

14.6. Тенденції розвитку активних пристроїв

Загальною тенденцією розвитку активних пристроїв є перенесення функцій пристроїв, що працюють на вищих рівнях протоколу у пристрої нижчих рівнів. У цьому випадку поліпшуються продуктивність та сервісні можливості таких пристроїв.

Наприклад, серед старших моделей виділяють *сегментувальні концентратори*, які здатні розділити свої порти на фіксовану кількість груп, кожна з яких утворює єдиний домен колізій. Перепускна здатність такого концентратора збільшується порівняно з аналогічним без сегментації.

Провідною тенденцією розвитку комутаторів є збільшення їхніх можливостей шляхом виконання функцій маршрутизації та підтримки віртуальних локальних мереж. **Комутація третього рівня** дає змогу відчутно збільшити перепускну здатність складних корпоративних мереж (див. Д.1.3 та розділ 19).

Бібліографія та джерела

1. *Барабанов С, Коростелин А., Крюков С.* Компьютерные сети: вчера, сегодня, завтра //Компьютерпресс. 1997. №2, 3. С. 152–158, 158–162.
2. *Барсков А.Г., Фоминов О.С.* Передовые технологии: Layer 3 switching // Сети и системы связи. 1997. № 8, 9.
3. *Бейкер Ф.* Как работают маршрутизаторы? // LAN Magazine.1997. № 2.
4. *Ганьжа Д.* Мосты в локальных сетях // LAN Magazine. 1997. № 2.
5. *Кульгин М.* Построить сеть, посадить дерево... // LAN Magazine. 1997. № 1.
6. *Шатт С.* Мир компьютерных сетей. К.: BHV, 1996.

ДОДАТКИ ДО РОЗДІЛУ 14

Д.14.1. Протокол залишкового дерева

Однією з проблем, що виникають під час побудови складних мереж з багатьма комутаторами, є можливість виникнення циклів передавання інформації. Вирішити її дає змогу протокол залишкового дерева **STP** (Spanning Tree Protocol), інколи його називають ще 'алгоритмом' (STA). Протокол STP розроблений DEC та стандартизований IEEE-802.1d. Він дає змогу ліквідувати фізичні та логічні петлі в мережах, побудованих з використанням комутаторів, а крім того, автоматично переконфігуровувати систему у випадку збоїв обладнання. Сьогодні підтримка STP реалізована в комутаторах багатьох фірм.

Розглянемо мережу з трьох комутаторів, сполучених між собою (рис. Д.14.1.1). Нехай станція *А* генерує циркулярне повідомлення. Його одержать комутатори *Б* та *В*, обміняються ним і знову перешлють комутатору *А* (циркулярні повідомлення передаються у всі вихідні порти, крім того порту, з якого вони прийняті). Утворюється 'шторм повідомлень'. Аналогічна проблема виникає і на етапі, коли комутатори ще не побудували свої маршрутні таблиці. Нехай станція *А* передає повідомлення станції *Б*. Унаслідок цього комутатори *Б* та *В* одержать повідомлення від *А*, змінять свої маршрутні таблиці, передадуть повідомлення один одному, знову змінять свої таблиці і так далі. У результаті таблиці будуть некоректними. Вирішити проблему циклів можна, якщо визначити тільки один шлях між кожною парою комутаторів.

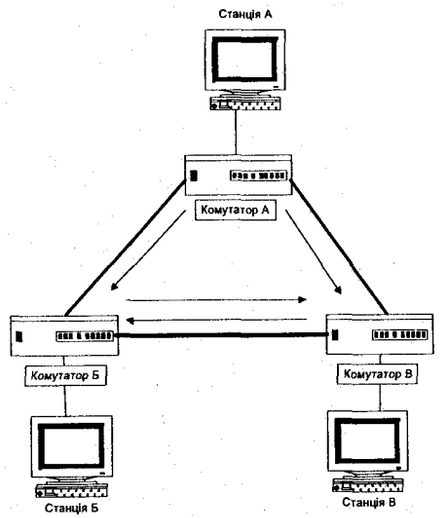


Рис. Д.14.1.1. Виникнення 'шторму повідомлень'.

Реалізувати STP в мережі можна, якщо його підтримуватимуть усі комутатори. Під час роботи з алгоритмом STP комутатори обмінюються інформацією – пакетами **BPDU** (Bridge Protocol Data Unit). Пакети розміщуються у складі кадрів канального рівня (рис. Д.14.1.2).

Значення полів такі:

- *протокол ID* – ідентифікатор протоколу дорівнює 0;
- *версія* – поле версії протоколу дорівнює 0;
- *тип повідомлення* дорівнює 0, якщо робота нормальна, і 80h, якщо є повідомлення про зміну топології;
- *прапорці*; байт використовує два біти; перший сигналізує про зміни у топології (TC – Topology Change); восьмий підтверджує приймання пакета з *TC*=1 (позначають TCA – Topology Change Acknowledgment);
- *кореневий ID* – ідентифікатор кореневого комутатора; поле складається з восьми байтів; перші два байти – ідентифікатор комутатора, решта шість – його MAC-адреса;
- *вартість шляху до кореня* відображає сумарну вартість шляху до кореневого комутатора;
- *ідентифікатор комутатора*, що надіслав повідомлення;
- *ідентифікатор порту комутатора*, звідки спрямоване повідомлення;
- *вік повідомлення* – час, що минув з моменту відсилання повідомлення про зміну топології;
- *максимальний вік* – час знищення повідомлення;
- *тривалість вітання* (Hello time) – проміжок часу між відсиланнями повідомлень кореневим комутатором;
- *затримка переходу* – час, який комутатори повинні чекати, перш ніж перейти у новий стан у випадку змін топології.

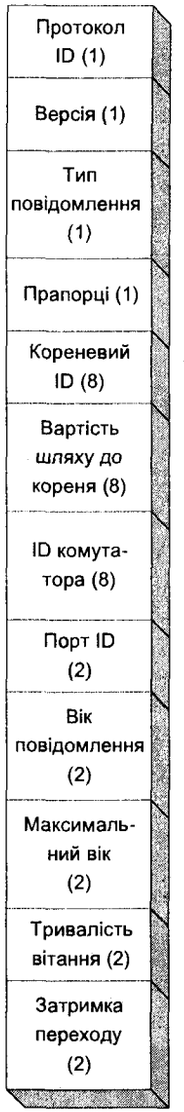


Рис. Д.14.1.2. Структура BPDU-пакета.

Для успішної роботи протоколу адміністратор попередньо повинен визначити два типи параметрів: ідентифікатор комутатора (див. вище) та вартість кожного його порту. Вартість портів можна задавати вручну або автоматично, присвоюючи довільне число від 0 до 65535, що зворотно пропорційне до швидкості передавання порту. Це число обчислюють за формулою

Вартість порту = 1000/(швидкість передавання порту, Мбіт/с).

Наприклад, вартість порту 10Base-T – 100, 100Base-TX –10, FDDI – 10, Token Ring – 250 або 63, T1 – 651, RS232C зі швидкістю 56 Кбіт/с – 17857.

На початку роботи алгоритму вибирають кореневий комутатор шляхом циркулярного розсилання BPDU-пакетів на всі порти комутатора. Кожен комутатор рекламує себе як кореневий і розміщує свій ідентифікатор у полях *кореневий ідентифікатор* та *ідентифікатор комутатора*.

Будь-який комутатор, одержавши пакет з ідентифікатором, що менший від його власного, починає розсилати пакети з цим ідентифікатором, припинивши розсилати зі своїм. У результаті кореневим стає комутатор з найменшим ідентифікатором (рис. Д.14.1.3).

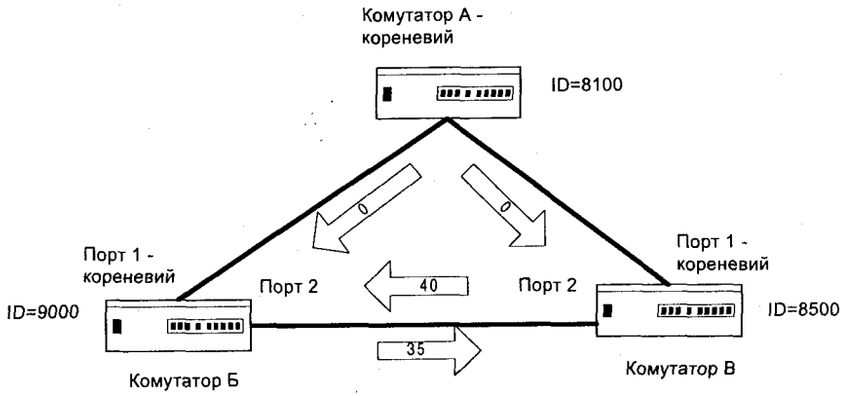


Рис. Д.14.1.3. Алгоритм залишкового дерева.

Другим кроком роботи алгоритму є визначення вартості портів. Кореневий комутатор починає надсилати BPDU-пакети на всі вихідні порти. У їхньому полі *вартість шляху до кореня* спочатку є нуль. Інші комутатори додають вартості своїх портів і розсилають пакети далі. Це дає змогу кожному комутатору визначити свій кореневий порт, через який можна потрапити в кореневий комутатор з найменшою вартістю. У наведеному вище прикладі комутатори *Б* та *В* додають вартості своїх портів (35 та 40) та пересилають повідомлення один одному. Після аналізу цих повідомлень комутатор з найбільшою вартістю шляху до кореня переводить свій порт у блокований стан. Порт, що перебуває в цьому стані, не передає кадри, однак продовжує приймати та опрацьовувати BPDU-пакети. Порт *2* комутатора *Б* стає призначеним (designated). Отже, незважаючи на те, що *Б* передаватиме кадри через порт *2*, їх відсікатиме комутатор *В*. Усі порти кореневого комутатора є призначені.

Загалом порт комутатора, що працює згідно зі стандартом IEEE-802.1d, може перебувати в одному з чотирьох станів.

1. **Блокований** (blocking state) порт не бере участі в нормальних операціях навчання, фільтрування та передавання, не передає трафік. Однак він приймає та аналізує BPDU-пакети, однак не передає їх далі. Якщо порт не одержить повідомлення протягом визначеного часу, він перейде у стан прослуховування. Кореневі та призначені порти у блокованому стані не бувають.

2. **Прослуховування** (listening state). Порт прослуховує BPDU-пакети для з'ясування потреби переходу в блокований стан або у стан навчання. Порт не бере участі в операціях з визначення розміщень станцій, фільтрування та передавання інформації користувачів. Стан прослуховування є тимчасовим і потрібний для мінімізації некоректної інформації у випадку переконфігурації STP. Тривалість перебування порту в цьому стані дорівнює значенню поля *затримка переходу* (за замовчуванням 15 с).

4. **Навчання** (learning state). Порт готується до переходу у стан передавання. Комутатор запам'ятовує розміщення станцій та оновлює адресну таблицю. Тривалість навчання дорівнює тривалості прослуховування.

5. **Передавання** (forwarding state). Порт бере участь у всіх діях комутатора. Він аналізує розміщення станцій, фільтрує дані, передає трафік користувача в обох напрямах. У цьому стані можуть перебувати тільки кореневі та призначені порти.

Після створення нової топології комутатор починає періодично розсилати BPDU-пакети. Інтервал між розсиланнями задає адміністратор під час налаштування (цей параметр передається у полі *тривалість вітання*, за замовчуванням – 2 с). Інші комутатори, що одержали цей пакет, збільшують поле *вік повідомлення*, доки воно не набуде максимального значення (максимальний вік) і тоді пакет знищується.

Протокол STP виконуватиме переконфігурацію у таких випадках: вийде з ладу кореневий комутатор або лінія зв'язку, своєчасно не одержане повідомлення від кореневого комутатора та ін. Кожен комутатор очікує одержання BPDU-пакета до закінчення 'максимального віку', в іншому випадку відбувається переконфігурація. Комутатор генерує BPDU-пакети з типом 80h. Крім того, відбуваються процеси вибору кореневого комутатора, призначених та блокованих портів, приєднання резервних ліній.

Варіанти резервування: це використання резервних ліній або резервних комутаторів.

Одним з недоліків класичного протоколу STP є непристосованість до архітектури віртуальних мереж. Єдиний шлях, який регламентує цей протокол, не задовольняє вимог різних віртуальних мереж. Фірма **Cisco** запропонувала варіант протоколу *Autonomous Spanning Tree*, який дає змогу для кожної віртуальної мережі підтримувати окреме дерево. Водночас, доки не прийняті стандарти щодо віртуальних мереж, такі розробки становлять тільки академічний інтерес.

Переваги протоколу STP такі: він дає змогу створювати великі стійкі до збоїв мережі; підтримує тільки один шлях між кожною парою станцій; гарантує надходження кадрів у послідовності передавання; ліквідує циркулярне передавання та зациклювання; займає невеликий відсоток смуги перепускання.

Його недоліки: вартість комутаторів з STP велика; він задіює додаткові порти комутаторів; під час реконфігурації мережа не передає інформацію; між довільною парою станцій може бути не більше семи комутаторів.

Д.14.2. Принципи роботи маршрутизаторів

Маршрутизатори, як і комутатори, працюють з таблицями адрес, однак адресують мережі. Архітектура маршрутизатора з інтеграцією послуг показана на рис. Д.14.2.1.

Як бачимо, у маршрутизаторі можна виділити два рівні. **Рівень маршрутизації** працює у фоновому режимі. Його завдання – підтримувати актуальність маршрутних таблиць, керувати трафіком, надавати деякі необов'язкові сервіси. Його робота має нижчий пріоритет порівняно з роботою рівня комутації.

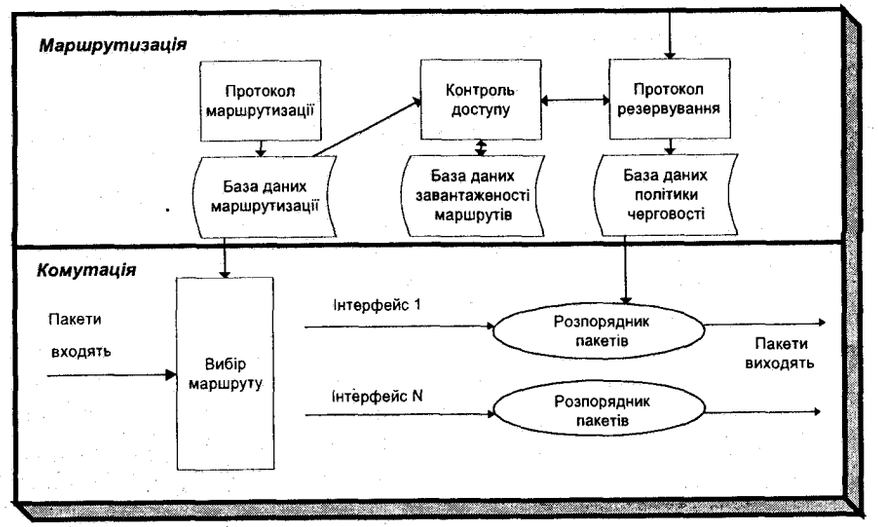


Рис. Д.14.2.1. Архітектура маршрутизатора.

Рівень комутації призначений для якнайшвидшого визначення маршруту проходження одержаного пакета та спрямування його на певний вихідний інтерфейс у чергу розпорядника пакетів. Швидкодія роботи рівня комутації визначає швидкодію маршрутизатора.

База даних маршрутизатора – це набір маршрутів. Рядки цього набору містять таке:

- задіяні адреси або множини задіяних адрес мережі;
- інформацію, обчислену протоколом маршрутизації (метрики, ваги маршрутів та ін.);
- інформацію, потрібну для того, щоб переслати пакет на один маршрутизатор ближче до одержувача.

Найчастіше зазначають дані про вихідний інтерфейс та адресу наступної системи.

Роботу рівня комутації підтримують такі процеси: вхідний драйвер, процеси вибору маршруту та керування чергою, вихідний драйвер. Шлях пакета намагаються зробити оптимальним щодо швидкості. Рівень комутації аналізує CRC, адреси, визначає адресу вихідного інтерфейсу згідно зі своїми таблицями, може дефрагментувати пакети, записувати в пакет свою адресу або часову позначку. Після опрацювання пакета у модулі вибору маршруту його спрямовують у чергу визначеного вихідного інтерфейсу. Розпорядник пакетів визначає момент їх відправлення.

Дисципліна відправлень. Найчастіше підтримується черга **FIFO** (First-In, First-Out). Це просто, однак не оптимально. У випадку переповнення черги відкидаються останні пакети, як звичайно, декількох різних абонентів. Втрату пакетів вони інтерпретують як сигнал про потребу зменшити швидкість генерації. У результаті навантаження різко зменшується. Потім ті ж абоненти проаналізують завантаження мережі і вирішать збільшити швидкість передавання. Переповнення повториться. Черги **RED** (Random Early Detection) пом'якшують ефект від втрати

пакетів, відкидаючи їх не з кінця черги, а випадково. Використання **черг з пріоритетами** призводить до того, що пакети з низьким пріоритетом взагалі не передаються або втрачають свою актуальність. Черги згідно з класом **CBQ** (Class Based Queuing) – це алгоритм, у якому трафік поділяється на пакети деяких класів. Кожен клас має свою чергу і йому гарантується певна перепускна здатність каналу.

Вхідні та вихідні драйвери – це програми та чіпи для приймання та передавання пакетів. Під час роботи вони по-різному розглядають та враховують різні типи каналів. Розрізняють такі типи каналів:

- *локальні мережі.* Необхідне визначення адрес канального рівня за мережевими адресами. Потрібно мати унікальну адресу мережевого рівня;
- *двопунктові канали* (PPP, HSSI). Прямо сполучають двох учасників. Деякі архітектури маршрутизації розглядають це як сполучення між двома половинами одного маршрутизатора. Немає потреби в адресах. Канал повністю контролюється;
- *канали нерегулярного доступу.* Асинхронні комутовані канали або ISDN. Подібні до двопунктових каналів, проте у випадку недоступності каналу потребують набору номера;
- *мережі загального доступу з віртуальними сполученнями.* ATM, X.25, Frame Relay. Розглядають як локальні мережі або сукупність двопунктових сполучень. Кожна система має свою адресу, однак вона відповідає адресі віртуального сполучення. Для одного віртуального сполучення не треба адрес (подібність до двопунктового інтерфейсу), повний контроль параметрів передавання.

Д.14.3. Комутація третього рівня

Походження терміна

У класичному розумінні схеми передавання даних у КМ комутатори працюють як багатопортові мости на канальному рівні. Вони не виконують функцій маршрутизації. На мережевому рівні працюють маршрутизатори. Як звичайно, маршрутизатори коштують дорожче і спричинюють більшу затримку в передаванні, ніж комутатори. Така схема добре працювала у мережах робочих груп, де сервер був у тому самому сегменті, що й користувачі. В такій ситуації правильним було емпіричне співвідношення розподілу потоків 80/20 (80 відсотків інформації циркулює всередині сегмента, а 20 – іде назовні). Із запровадженням систем, які реалізують концепцію розподілених обчислень, збільшенням розміру мереж, можливостей роботи з багатьма віддаленими серверами одночасно, роботою web-систем пропорція у розподілі потоків докорінно змінилася. Можна сказати, що вона стала загалом непередбачуваною і залежить від комплексу завдань, які вирішуються в системі, поведінки користувача. Частково цю проблему вирішують запровадженням комутації локальних мереж. Водночас великі міжмережеві потоки, висока вартість маршрутизаторів, значна затримка інформації в них зумовлюють потребу перенесення частини функції маршрутизації у дешевші та швидкіші комутатори.

Технології, які реалізують функції мережевого рівня у комутаторах мають загальну назву ***комутації третього рівня*** *(Layer 3 switching).*

Першими пристроями, які можна вважати комутаторами з маршрутизацією, є продукти фірм Synernetics та Alantec, які з'явилися на початку 90-х років. Кожен кадр даних у них міг бути комутований або маршрутизований. Комутатор аналізував адреси відправника та одержувача. Якщо вони належали одній локальній мережі, відбувалася комутація кадру, в іншому випадку – маршрутизація.

Апаратні підходи

Комутацію третього рівня реалізують у двох типах пристроїв:
- комутаторах з маршрутизацією;
- комутаторах з модулями маршрутизації.

У першому типі функція маршрутизації органічно вбудована в конструкцію комутатора. В інших можна виділити окремий модуль, що займається маршрутизацією та обмінюється інформацією з іншими модулями по внутрішній шині. Процеси комутації та маршрутизації тут значно менше інтегровані, ніж у комутаторах з маршрутизацією. Модулі маршрутизації часто будують на базі автономних маршрутизаторів зі стандартними інтерфейсами. Швидкість обміну таких модулів з центральною шиною комутатора значно менша, ніж внутрішня швидкість передавання інформації шиною комутатора.

Продуктивність *комутатора визначають кількістю пакетів за секунду, яку здатний маршрутизувати комутатор. Якщо комутатор здатний працювати з номінальною швидкістю фізичної мережі (наприклад 100 Мбіт/с), то кажуть, що досягається* ***швидкість середовища*** *(wire speed) і говорити про подальше збільшення швидкості недоцільно, оскільки швидкість передавання вже буде обмежена швидкістю фізичної мережі.*

У комутаторах CoreBuilder 6000, 2500 фірми 3Com в апаратній архітектурі одночасно використано мікросхеми ASIC (Application Specific Integrated Chip), процесори RISC та CISC. У цьому випадку комутацію пакетів та первинний аналіз виконують найшвидкіші ASIC-мікросхеми, RISC-процесори зайняті маршрутизацією, а CISC – керуванням.

У комутаторах **PowerHub** (FORE Systems) всю роботу з комутації та маршрутизації виконують декілька RISC-процесорів, що працюють паралельно.

Комутатор **Switch Node** (Bay Networks) може працювати у режимі навчання IP Autolearn. У цьому випадку він будує маршрутну таблицю для IP-адрес без застосування якогось з протоколів маршрутизації. Такий комутатор можна приєднати у будь-яку мережу, незважаючи на протокол маршрутизації, який у ній використано.

У продукті **8210 Nways MSS Server** (IBM) реалізовано клієнт-серверний підхід до реалізації маршрутизації, тобто функції вибору маршруту та безпосереднього пересилання трафікурозділені. Вибір маршрутів виконують сервери маршрутів, а пересилання пакетів – клієнти. Клієнти запитують у сервера про маршрутну інформацію тільки один раз – під час

пересилання першого пакета сеансу. У подальшому маршрут кешується і використовується для передавання всіх інших пакетів.

У комутаторі **Cisco 7500** реалізована технологія Net Flow, в якій за адресними параметрами пакета обчислюється значення геш-функції. Висновок про маршрутизацію кожного одержаного пакета робиться на підставі обчислення для нього геш-значення та шукання відповідного значення у геш-таблиці.

Алгоритми роботи пристроїв

Сьогодні є п'ять головних підходів до організації комутації третього рівня.
- Міжрівневе відображення (multilayer mapping).
- Використання функції переспрямування ICMP.
- Використання призначеного сервера.
- Переконфігурування клієнтських станцій та використання протоколу ARP.
- Використання DHCP.

У деяких підходах комутатор аналізує кожен пакет і приймає рішення про його комутацію або маршрутизацію, в інших аналізує тільки перший пакет сеансу. IP-адреса у цьому випадку відображається у MAC-адресу, а для наступних пакетів за цією адресою відбувається комутація.

Головна мета комутації третього рівня – 'змусити' станцію повірити в те, що вона зможе зв'язатися з будь-якою іншою станцією без допомоги маршрутизатора. Розглянемо кожен підхід детальніше.

Міжрівневе відображення (multilayer mapping (MLM)) потребує наявності комутаторів, які відображають адреси третього рівня в адреси другого. Комутатори містять таблиці топології мережі. За ними на початку кожного сеансу можна побудувати віртуальне сполучення, а потім спрямовувати наступні пакети цими сполученнями вже з використанням комутації. Схеми комутації з MLM можуть ґрунтуватися на розподілі потоків або ж на відомій топології мережі.

Іншим підходом є технологія **Ipsilon IP Switching**. Комутатори цієї технології визначають тривалі потоки в мережі (передавання файлів, робота telnet, web) і виділяють для них віртуальні сполучення, за якими відбувається комутація. У дуже великих мережах кількість потоків може перевищити кількість наявних віртуальних сполучень.

У схемах, що ґрунтуються на топології мережі, рішення про спрямування пакета приймається на підставі адресної інформації в цьому пакеті. Прикладом такої технології є **Tag Switching** фірми Cisco. Адреси третього рівня відображаються в додаткові позначки (теги), за якими і відбувається комутація (рис. Д.14.3.1).

Спільним недоліком усіх технологій міжрівневого відображення є потреба наявності граничних пристроїв, які б узгоджували вхідний у мережу потік з деталями реалізації MLM.

Системи з **ICMP-переспрямуванням** використовують здатність кожного маршрутизатора переспрямувати потік клієнта на іншу адресу. Прикладом цього підходу є технологія **PowerIP** фірми RND Networks. Вона не потребує переналагодження кінцевих вузлів. Коли станція *А* передає для станції *Б* пакет, то він проходить через маршрутизатор та маршрутизується за класичною схемою. Водночас комутатор змінює маршрут передавання трафіку цього сеансу, використовуючи спеціальну команду протоколу ICMP (переспрямування, ICMP-redirect). У

цій команді задається для станції *Б* віртуальна адреса, яка належить одній зі станцією *А* мережі, та MAC-адреса станції *Б*. Для наступних пакетів сеансу відбувається комутація. Віртуальні адреси беруться з деякого пулу адрес динамічно. Після закінчення набору 'вільних' адрес пакети маршрутизуються за класичною схемою. Недоліком такої технології є обмеженість масиву вільних IP-адрес мережі.

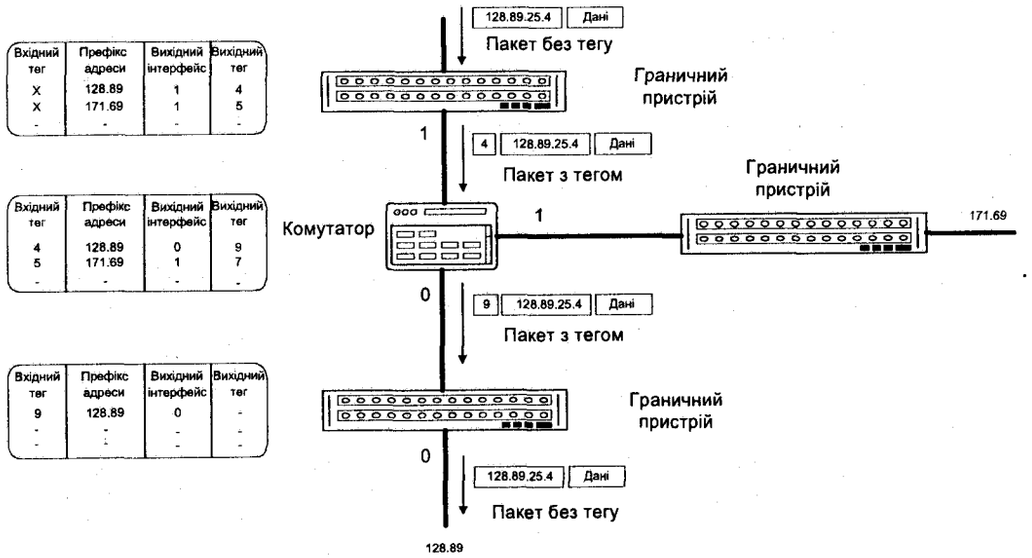


Рис. Д.14.3.1. Технологія 'Tag Switching'.

У системах зі **спеціальним призначеним сервером маршрутизації** шляхи у мережі розраховує цей сервер. Системи, як звичайно, використовують протокол **NHRP** (Next Hop Routing Protocol). Станція, яка хоче передавати дані іншій станції, надсилає NHRP-запит найближчому серверу маршрутизації. Цей запит містить MAC- та IP-адреси джерела та ідентифікатор віртуальної мережі (VLAN ID). Якщо сервер знає шлях до адресата, то запит передається йому. Адресат формує NHRP-відповідь, у яку записує свою адресну інформацію. Відповідь передається джерелу напряму, а не через сервер. Наступні пакети сеансу комутуються без участі сервера. Якщо маршрутний сервер не знає шляху до адресата, він опитує інші маршрутні сервери. Недоліком такої технології є те, що протокол NHRP повинні підтримувати всі компоненти мережі, а багато наявного обладнання його не підтримує. Підхід з призначеним сервером підтримують фірми IBM, 3COM.

У схемах з використанням протоколу ARP клієнтські станції переналагоджуються таким чином, щоб відсилати ARP-запит навіть тоді, коли адресат є в одній локальній мережі з відправником. Пакет запиту перехоплюється комутатором. Якщо адресат та відправник є в одній локальній мережі, то комутатор повідомляє MAC-адресу адресата. В іншому випадку він

повідомляє MAC-адресу свого вихідного порту, через який можна зв'язатися з адресатом. Такий підхід використовують у технології **IP Packet Switching** фірми Digital та технологіях фірми Cabletron. Недоліком його є ручне переналагодження великої кількості клієнтських станцій.

У технології **DirectIP** фірми Nbase переналагодження робочих станцій відбувається з використанням протоколу DHCP. Маски підмереж задають так, щоб станція сприймала, що її адресат перебуває з нею в одній мережі. ARP-запит станції *А* перехоплює комутатор. Він визначає за IP-адресою станції *Б*, чи дозволено сполучення та, якщо дозволено, спрямовує станції *А* MAC-адресу станції *Б*. У подальшому відбувається комутація. У цій реалізації нема ручного переналагодження станцій. Початкову топологію мережі вводять на центральному комп'ютері, а пізніше розсилають по всій мережі. Програма керування мережею здатна навчатися та стежити за змінами у топології мережі. Під час DHCP-переналагодження мережі до пакета запиту додається вся необхідна інформація для організації комутації третього рівня. Після початкового переналагодження весь інформаційний потік комутується зі швидкістю носія (wire speed).

Розділ 15

ЛОКАЛЬНА МЕРЕЖА ETHERNET

Локальна мережа Ethernet. Історія її створення. Варіанти топологічної структури. Характеристики кабельних з'єднань 10Base-5, 10Base-2, 10Base-T, 10Base-F. Головні параметри та характеристики мережі. Адаптери мережі. Перспективи та тенденції розвитку.

15.1. Загальна характеристика та історія створення

ЛМ Ethernet найпростіше можна визначити як шинну мережу з МДКН/ВК (див. розділ 7). Вона проста, дешева, надійна та ефективна, має високу швидкість передавання даних і завдяки цьому стала найпоширенішою. Деякі комп'ютери, наприклад IBM PS/1, а також потужні робочі станції Apollo (Hewlett-Packard), Sun та інші вже мають адаптер Ethernet у стандартній конфігурації. У деяких розробках адаптер Ethernet починають інтегрувати з материнською платою.

Перший лабораторний варіант Ethernet розробила фірма Xerox (відділення в Пало-Альто) ще в 1975 р.[1] У 1980 р. Xerox, DEC та Intel опублікували специфікацію Ethernet, яка охоплювала фізичний та канальний (MAC) рівні протоколу. Сьогодні мережа Ethernet схарактеризована в стандартах IEEE-802.3 та ECMA-82. Завдяки простоті, дешевості, здатності до масштабування Ethernet є лідером серед інших типів локальних мереж. Ця технологія продемонструвала значний потенціал розвитку та стала основою для технологій комутованого Ethernet, Fast Ethernet та Gigabit Ethernet (див. розділи 16, 19).

15.2. Варіанти кабельних з'єднань

Топологічна структура, параметри та вартість реалізації мережі Ethernet залежать від типу кабельного з'єднання. Сьогодні є кілька типів кабельних з'єднань. Їх маркують так:

NNNN Base-XX.

Перші цифри (NNNN) характеризують швидкість передавання, Мбіт/с, символи XX – максимальну довжину сегмента в сотнях метрів або середовище передавання. Мережа Ethernet звичайно складається з одного або кількох шинних сегментів, сполучених за допомогою повторювачів (repeaters) або концентраторів (hubs, linkbuilders).

[1] Термін Ethernet уперше згадано 22 травня 1973 р. в доповідній записці, яку склав Роберт Меткалф, співробітник дослідницького центру Xerox у Пало-Альто, Каліфорнія, сформулювавши головні принципи організації мережі Ethernet.

10 Base-5 – товстий Ethernet (Thick Ethernet)

Максимальна довжина одного сегмента (без підсилення сигналу) – 500 м. Кабель RG6 коштує дорого, однак має високу механічну стійкість. Для приєднання до мережі потрібні адаптери з AUI-роз'єднувачами та блоки трансиверів (приймача та передавача), які монтують безпосередньо на кабелі з проколюванням ізоляції (рис. 15.1) (див. розділ 3). На кінцях кабелю встановлюють узгоджувальні індуктивності – термінатори. Кабель RG6 важко прокладати, однак він ліпше захищений від завад порівняно з "тонким" Ethernet'ом, та сьогодні його поступово витісняють волоконно-оптичні кабелі. Історично "товстий" Ethernet був першим варіантом мережі.

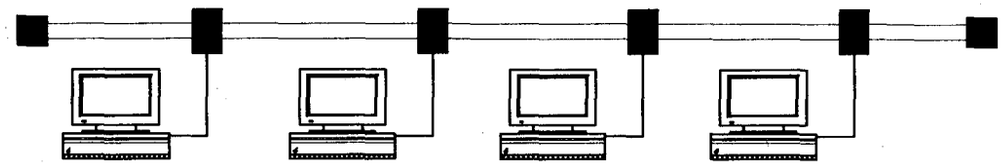


Рис. 15.1. Товстий Ethernet.

10Base-2 – тонкий Ethernet (Thin Ethernet, Cheapernet)

Максимальна довжина одного сегмента становить 185 м. Мережа має шинну багатосегментну топологію. Для приєднання станції до мережі використовують BNC Т-з'єднувач (рис. 15.2). У мережі застосовують дешевий кабель RG 58C/U. Цей кабель погано захищений від завад, контакти його приєднання до станцій ненадійні та незахищені від дій користувача. Порушення контакту спричинює розрив мережі. Сьогодні цей метод сполучення модифікований за допомогою EAD-технології, якою передбачено, що тонкий кабель з'єднує спеціальні гніздарозетки, заховані в стіні. Користувач приєднує свою станцію до мережі за допомогою шиекера. Кабелі приєднання можна відмикати від розетки без порушення мережі.

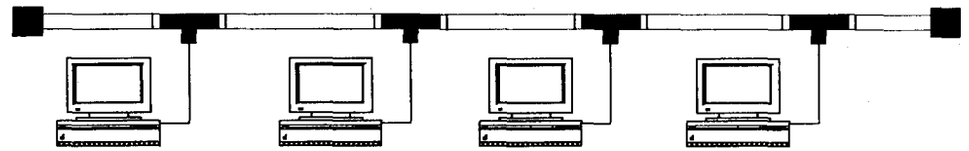


Рис. 15.2. Тонкий Ethernet.

10Base-T – Ethernet на скрученій парі (Twisted Pair Ethernet)

Топологія з'єднань – розподілена зірка (рис. 15.3). Максимальна віддаленість станції до концентратора – 100–160 м. Кабель дешевий та простий для прокладання. Цей тип кабелю

використовують в інших засобах зв'язку та мережах (Token Ring, Arcnet, RS232C, ISDN, телефон). Обмеження на відстань до концентратора, якщо концентраторів є достатня кількість, немає великого значення. Як концентратори можна використати багато різних пристроїв. Мережа на скрученій парі проста в обслуговуванні, експлуатації та діагностуванні пошкоджень. Вона поступово стає головним варіантом мереж Ethernet.

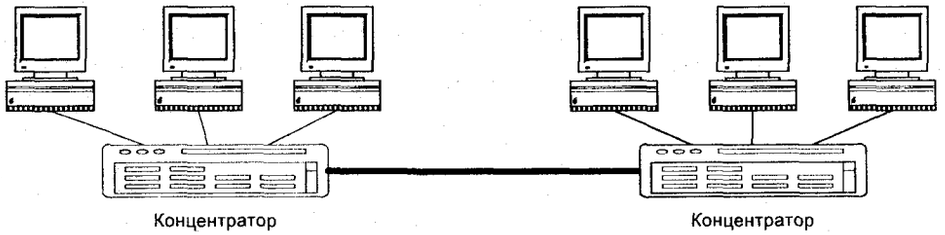


Рис. 15.3. Ethernet на скрученій парі.

Стандарт 10Base-T має декілька нових характеристик, пов'язаних з використанням концентраторів та можливістю їх інтелектуалізації. Наприклад, ним передбачено контроль за часом безперервного передавання даних з концентратора. Якщо концентратор передає довше визначеного часу, то передавання на деякий період припиняється. Реалізована також схема інтелектуальної фільтрації, яка дає змогу виділяти сигнал даних Ethernet з загального набору сигналів (телефон, ISDN та ін.). Як відомо, під час передавання скрученою парою сигнал спотворюється. Тому розроблено спеціальний метод попередньої корекції, в якому сигнал спеціально спотворюється до початку передавання, щоб компенсувати його зміни під час передавання.

10Base-F – волоконно-оптичний Ethernet (optical fiber Ethernet)

Мережа побудована на волоконно-оптичному кабелі, що забезпечує повну гальванічну ізоляцію. Максимальна відстань передавання – до 2 км. Кабель легкий, має менші габарити, ніж товстий Ethernet, однак дорожчий від нього. Забезпечує тільки двопунктове сполучення (point-to-point connection), тому його використовують, як звичайно, тільки для магістральних ліній як доповнення до Ethernet на скрученій парі (рис. 15.3). Для приєднання волоконно-оптичного кабелю потрібні волоконно-оптичні Ethernet роз'єднувачі та волоконно-оптичні трансивери. Розповсюдженню мереж на волоконно-оптичних кабелях перешкоджає низька механічна стійкість кабелю.

Дуплексний Ethernet

Наприкінці 1993 р. фірма Kalpana запровадила дуплексну технологію Ethernet. Ця мережа складається з двох каналів, що мають швидкість передавання 10 Мбіт/с. Один з них використовують для приймання, а інший – для передавання *двопунктовим сполученням*. Сумарна швидкість становить 20 Мбіт/с. Найбільшої ефективності дуплексного Ethernet можна досягти, якщо збалансувати завантаження обох напрямів. Водночас, якщо навіть розглядати передавання в одному напрямі, то вислідна перепускна здатність дуплексного Ethernet буде вищою, оскільки не виникає колізій. Типовий варіант використання дуплексного Ethernet – канал між комутатором та сервером.

Зазначимо, що, будуючи Ethernet, треба зважати на деякі обмеження (див. розділ 20).

15.3. Структура кадру та порядок роботи

Типова мережа Ethernet передбачає приєднання 1024 робочих станцій, діаметр мережі близько 1000 м (з повторювачами). У ній застосовують манчестерське кодування (див. розділ 3). Затримки передавання інформації для мережі Ethernet випадкові та залежать від загального навантаження. Якщо протягом перших десяти спроб передавання виникають колізії, то ці спроби відкладаються на випадковий період, який вибирається зі зростаючих інтервалів від 0–1 до 0–1023. Якщо у 16-й спробі кадр передати не вдалося, то станція відмовляється від передавання і повідомляє про це протокол верхнього рівня. Формат кадру мережі Ethernet показано на рис. 15.4.

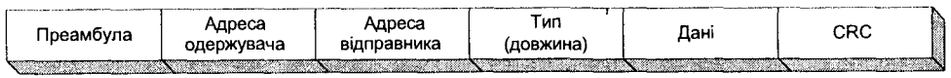


Рис. 15.4. Структура кадру мережі Ethrnet.

На початку кадру є *преамбула* (див. розділ 3). *Адреси одержувача* та *відправника* – це числа до 2^{47}, звичайно починаються з 0. Групові адреси починаються з 1. Поле *типу* специфікує протокол верхнього рівня, якому призначений кадр. Поле *даних* містить пакет верхнього рівня. Весь кадр захищено полем циклічної суми (CRC).

Мінімальна довжина кадру становить 64 байти, максимальна – 1518. Довжина кадру обмежена знизу тим, що тривалість передавання кадру у мережі згідно з вимогами стандарту IEEE-802.3 (для надійного виявлення колізій) не може бути меншою ніж подвоєна тривалість поширення сигналу між двома найвіддаленішими станціями. Отже, мінімальна довжина кадру обмежує довжину (діаметр) мережі. Визначення максимальної довжини кадру випливає з потреби зменшити колізії, оскільки як експериментально доведено, що в разі довжини кадру понад 1500 байт імовірність виникнення колізій різко збільшується.

На рис. 15.4 показано структуру кадру формату Ethernet II. Цей формат використовували у специфікації Ethernet фірм Xerox, DEC, Intel. У сучасних мережах, крім того, широко застосовують і формат Ethernet IEEE-802.3, запропонований у специфікації IEEE-802.3 (див. Д.15.1).

15.4. Адаптери мережі Ethernet

Адаптерні плати мережі Ethernet виробляє багато фірм. Зокрема:
фірма DEC виробляє адаптери Etherworks різних модифікацій;
Allied Telesyn – AT;
3COM – Etherlink;
Hewlett-Packard – Etherexpress;
Eagle – NE1000, NE2000.

15.5. Тенденції розвитку архітектури Ethernet

Сьогодні архітектура Ethernet – найпоширеніша в організації ЛМ. Така мережа проста в організації та експлуатації. Суттєві недоліки мереж Ethernet такі: нема гарантованої тривалості передавання кадру, невелика перепускна здатність при високих навантаженнях (в Ethernet-мережах реальна перепускна здатність не перевищує 50–60% від максимальної). Тому для організації магістральних ЛМ з високим трафіком доцільніше використовувати архітектуру FDDI, яка дає змогу виділити до 85% перепускної здатності каналу на передавання інформації користувача, а ціна її ненабагато вища від аналогічних за функціями комутованих мереж Ethernet.

Однак, незважаючи на недоліки, Ethernet-технологія завдяки простоті ідеальна для невеликих та середніх мереж. Власне для Ethernet-мереж сьогодні активно розвивають технології комутації локальних мереж та віртуальних ЛМ, що дає змогу зняти обмеження Ethernet щодо перепускної здатності (див. розділ 19). Крім того, широко застосовують і технології швидких Ethernet та подібних мереж (див. розділ 16). Поступово мережа Ethernet завдяки оптимальному співвідношенню вартість/продуктивність та простоті стає головним стандартом для локальних мереж.

Бібліографія та джерела

1. *Вейцман К.* Распределенные системы мини и микро ЭВМ / Пер с англ. М.: Финансы и статистика, 1982.
2. Локальные вычислительные сети. Принципы построения, архитектура, коммуникационные средства / Под ред. С.В. Назарова. М.: Финансы и статистика, 1994.
3. Локальные вычислительные сети. Технические и программные средства / Под ред. С.В.Назарова. М.: Финансы и статистика, 1994.
4. Локальные вычислительные сети. Организация функционирования, эффективность, оптимизация / Под ред. С.В. Назарова. М.: Финансы и статистика, 1995.
5. *Флинт Д.* Локальные сети ЭВМ: архитектура, принципы построения, реализация / Пер с англ. М.: Финансы и статистика, 1986.
6. *Шатт С.* Мир компьютерных сетей. К.: BHV, 1996.
7. *Metcalf R.M., Boggs D.R.* Ethernet: distributed packet switching for local computer networks // Communications ACM. 1976. Vol. 19. N 7.

ДОДАТОК ДО РОЗДІЛУ 15

Д.15.1. Типи кадрів Ethernet

Розрізняють дві специфікації Ethernet з різними типами кадрів. Історично першою була специфікація фірм Xerox, DEC, Intel. Її кадр називається Ethernet II і показаний на рис. Д.15.1.1.

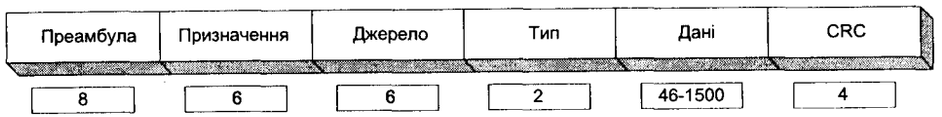


Рис. Д.15.1.1. Структура кадру Ethernet II.

Преамбула призначена для синхронізації кадру. У перших семи байтах вона містить код 10101010, а у восьмому байті – 10101011. Отже, восьмий байт є ознакою початку кадру.

Адреса *призначення* складається з шести байтів. Перший біт першого байта задає режим – індивідуальний або груповий. Якщо значення цього біта становить 0, то адреса є адресою конкретної станції мережі, якщо ж 1, то це групова адреса. Перші три байти в цьому випадку задають номер групи. Адресу зі всіма '1' використовують для циркулярних повідомлень.

Адреса *джерела* також має довжину шість байтів. Перший біт першого байта в ній – 0.

Поле *типу* протоколу задає протокол верхнього рівня, який працює з кадром. Такий розподіл дає змогу протоколам верхнього рівня виділяти власні потоки в загальному.

Дані мають змінну довжину. Мінімальна кількість даних – 45 байт, максимальна – 1500.

Поле *CRC (Cyclic Redundancy Check)* містить залишок, який обчислюють з використанням циклічного полінома 32 степеня (захист від спотворень).

Другий головний тип кадру відповідає специфікації IEEE-802.3 (див. рис. Д.15.1.2).

Рис. Д.15.1.2. Структура кадру IEEE-802.3.

Поля *преамбули* та *ознаки початку* повністю відповідають формату Ethernet II. Поле адреси *призначення*, крім аналогічних полів формату Ethernet II, у другому біті першого байта містить ознаку локальності/глобальності адреси. Окреме поле виділене для запису *довжини* поля даних. Поле *даних* може мати нульову довжину. Якщо ж це поле має довжину менше 46 байт, то кількість байтів до 46 доповнюється випадковими байтами в полі *Набивання*.

Крім того, перші байти даних завжди містять адресну та інформацію керування протоколу верхнього рівня IEEE-802.2. Це адреси пунктів доступу до послуг одержувача (DSAP) та відправника (SSAP) кадру, а також поле керування з одного байта.

Розділ 16

МЕРЕЖІ FAST ETHERNET, 100VG-ANYLAN, GIGABIT ETHERNET

Загальна характеристика, передумови появи сучасних швидкісних локальних мереж. Мережа Fast Ethernet: характеристика, топологія та обмеження. Архітектура фізичного рівня. Мережі 100Base-T4, 100Base-TX, 100Base-FX. Мережа 100VG-Anylan: загальна характеристика, стандартизація. Топологія, метод доступу та порядок роботи. Обмеження та параметри продуктивності мережі. Мережа Gigabit Ethernet.

16.1. Загальна характеристика та передумови появи сучасних швидкісних локальних мереж

Поява швидкісних локальних мереж Fast Ethernet та 100VG-Anylan зумовлена розвитком комп'ютерної технології, потребами сучасних застосувань щодо швидкодії та обсягів інформації для передавання. Специфікації Fast Ethernet та 100VG-Anylan з'явилися майже одночасно – на початку 90-х років. Специфікацію Fast Ethernet подано в комітет IEEE 802 у листопаді 1992 р. і затверджено як стандарт IEEE-802.3u. Стандартизацією Fast Ethernet займається комітет IEEE-802.3.

Специфікацію та перші пристрої 100VG-Anylan розробили фірми HP та AT&T у 1994 р. Стандарт було затверджено в червні 1995 р. Стандартизацією 100VG-Anylan займається спеціально створений для цього комітет IEEE-802.12. Сьогодні власником технології 100VG-Anylan є консорціум 100VG-Anylan Forum з фірм HP, AT&T, IBM, NTT, Asante та ін.

Обидві мережі можна схарактеризувати як ЛМ зіркової топології з теоретично можливою швидкістю передавання 100 Мбіт/с. Водночас між мережами є і суттєві відмінності.

16.2. Мережа Fast Ethernet

Характеристика, топологія мережі та її обмеження. Мережі Fast Ethernet мають топологію 'розподілена зірка', для сполучення використовують скручену пару різних категорій та концентратори. Замість скрученої пари можна застосовувати й волоконно-оптичні кабелі. Коаксіальні кабелі специфікація не підтримує. Відстань між мережевим концентратором та робочою станцією не повинна перевищувати 100 м. Максимальна відстань між двома станціями в мережі – 210 м. Між двома станціями не може бути більше двох повторювачів. За допомогою стекових повторювачіві, мостів, маршрутизаторів та комутаторів до мережі можна приєднати необмежену кількість сегментів Fast Ethernet (рис. 16.1).

Залежно від типу кабелю є кілька варіантів 100Base-T Fast Ethernet. Наприклад, у мережі 100Base-TX передавання даних відбувається двома парами дротів скрученої пари категорії 5, у мережі 100Base-T4 – чотирма парами дротів скручених пар категорій 3, 4, 5, у мережі 100Base-FX – волоконно-оптичним кабелем.

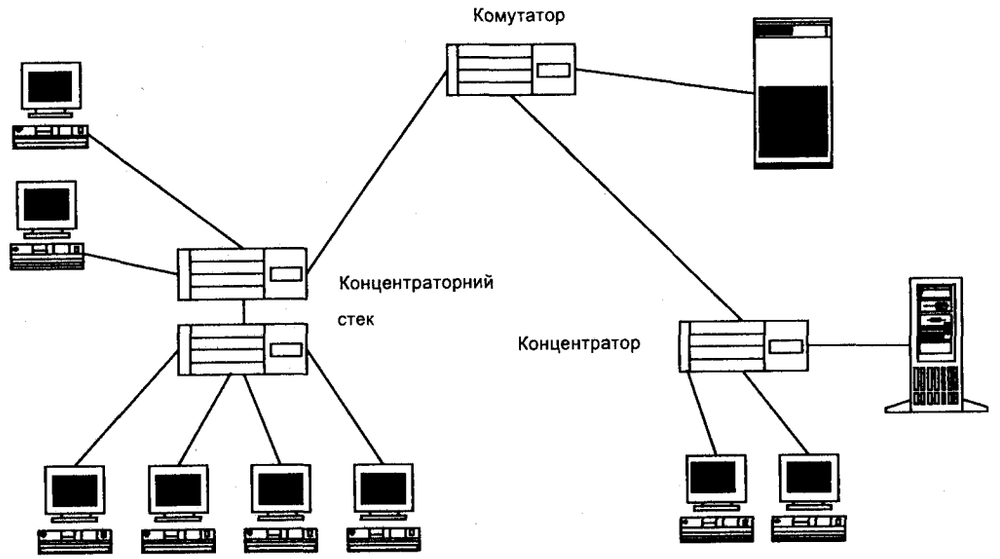


Рис. 16.1. Структура мережі Fast Ethernet.

Концентратори Fast Ethetnet. Центральним пристроєм мереж Fast Ethetnet є концентратор. Стандарт IEEE-802.3u визначає два класи концентраторів – I та II. Концентратори-повторювачі приймають сигнал на одному з портів та ретранслюють його на всі інші порти. Ця операція спричинює деяку затримку у поширенні сигналу. Параметр затримки визначений стандартом для кожного з класів.

Повторювачі класу I повністю декодують аналоговий сигнал, перетворюючи його у цифрову форму. Тому вони можуть мати порти різних форматів 100Base-T4, 100Base-TX, 100Base-FX. Їх ще називають трансляційними повторювачами. Концентратори класу II просто ретранслюють аналоговий сигнал на всі вихідні порти, крім порту, з якого він надійшов. З цього випливає, що затримка сигналу в концентраторах класу II менша і концентратори класу II можуть мати порти тільки одного типу.

Два концентратори класу II сполучають через спеціальний **uplink**-порт (рис. 16.2), що розміщений на одному концентраторі (з інтерфейсом MDI-X), та звичайний порт, що є на другому (з інтерфейсом MDI). Довжина з'єднувального кабелю – до 5 м.

Один сегмент мережі може містити концентратори тільки одного типу. В сегменті може бути один концентратор класу I або два концентратори класу II.

Концентратори класу I можна сполучати у стекову структуру, однак не через uplink-порт, а за допомогою внутрішніх шин концентраторів. Повторювачі класу II не утворюють стекових структур, оскільки мають більші обмеження щодо затримки кадрів. Якщо у стек додається новий концентратор, то приймають, що діаметр сегмента збільшується на 10 м. Як звичайно, максимальна кількість концентраторів у стеку не перевищує восьми.

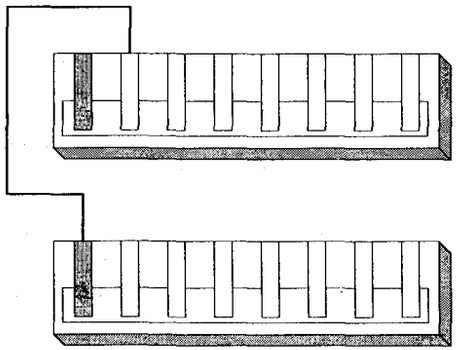


Рис. 16.2. Сполучення двох концентраторів.

Правила побудови мережі Fast Ethernet. Чим зумовлені обмеження щодо довжини сегмента та кількості концентраторів у ньому? Щоб відповісти на це питання, треба розглянути структуру затримок у сегменті.

Тривалість поширення сигналу на відстань 100 м скрученою парою становить 0.55 мкс та не залежить від швидкості передавання даних у мережі. Тривалість затримки у концентраторі – приблизно від 0.35 до 0.7 мкс залежно від класу концентратора. Мережева плата спричинює затримку в 0.25 мкс. *Для коректної роботи мережі Ethernet треба, щоб подвоєна тривалість передавання сигналу від одного краю сегмента до іншого не перевищувала тривалості передавання кадру мінімальної довжини.* Якщо ця умова не виконуватиметься, то тривалість колізії буде дорівнювати тривалості передавання кадру найменшої довжини, що у мережі 100Base-T становить 5.12 мкс.

На підставі наведеного аналізу структури затримок можна виділити такі коректні структури мереж:

• один концентратор класу I. Максимальна відстань між станціями – 200 м;

• два концентратори класу II, сполучені п'ятиметровим кабелем. Максимальна відстань між станціями – 205 м;

• один концентратор класу I з портами для скрученої пари та волоконно-оптичних кабелів. Максимальна відстань між станціями, приєднаними до різних типів кабелю, – 289 м (100+189);

• один концентратор класу I з портами для волоконно-оптичних кабелів. Максимальна відстань між станціями – 320 м (100+220).

Стандарт IEEE-802.3u передбачає дві моделі для розрахунку та побудови сегмента мережі:

• модель 1 передбачає, що всі елементи мережі вносять максимальні визначені стандартом для цих типів елементів затримки;

• модель 2 побудована на реальних затримках, однак має складні методики розрахунку цих затримок, які доцільно виконувати, якщо параметри мережі наближаються до максимально допустимих.

У моделі 1 передбачено такі топологічні обмеження:

• довжина скрученої пари довільної категорії не може бути понад 100 м;

• довжина відрізка волоконно-оптичного кабелю не повинна перевищувати 412 м.

Архітектуру фізичного рівня мережі розглянемо, порівнюючи її з архітектурою 10Base-T (рис. 16.3).

У 10Base-T нижче MAC-підрівня канального рівня на фізичному рівні є *підрівень фізичних сигналів* ***PCS*** *(Physical Coding Sublayer)*, який перетворює сигнал MAC-підрівня в сигнал манчестерського коду. PCS закінчується стандартним **AUI** (Attachment Unit Interface) – інтерфейсом, який сполучає робочу станцію з приймачем-передавачем (MAU). MAU (Media Access Unit) складається з блока керування передаваннями і виявлення конфліктів **PMA** (Physical Media Attachment) та інтерфейсу з конкретним передавальним середовищем **MDI** (Media Interface). Отже, стандарт 10Base-T допускає використання різних кабелів.

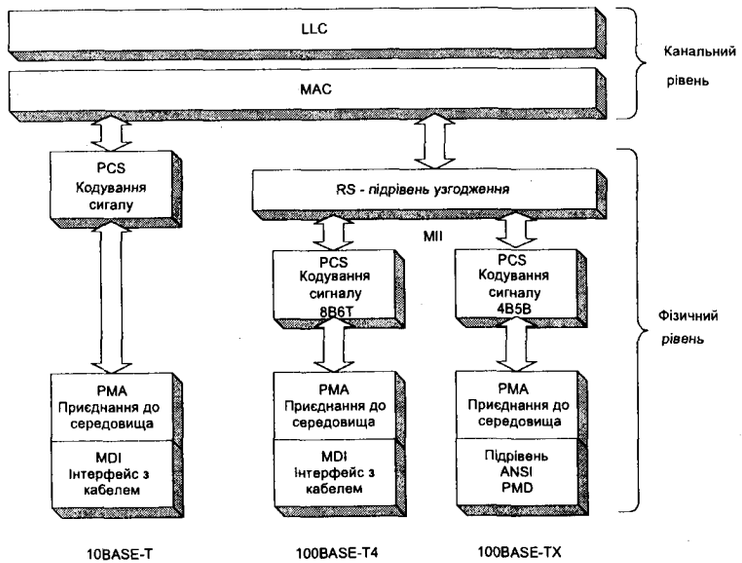


Рис. 16.3. Архітектура фізичного рівня.

У 100Base-T, на відміну від 10Base-T, можливе передавання не тільки через різні передавальні середовища, але й з використанням різних алгоритмів кодування. Для цього між MAC- та PCS-підрівнями реалізовано спеціальний *підрівень узгодження* ***RS*** *(Reconciliation Sublayer)*

з інтерфейсом **MII** (Media Independent Interface). RS перетворює абстрактні повідомлення MAC-підрівня в послідовність півбайтів і передає їх через MII нижньому підрівню. Є різні реалізації PCS залежно від алгоритму кодування інформації (8B6T або 4B5B).

Отже, стандарт 100Base-T – це наявний стандарт IEEE-802.3, доповнений функціональними блоками RS/MII. У деяких пристроях 100Base-T є спеціальний блок, який аналізує швидкість передавання даних. Це дає змогу суміщати передавання даних 10Base-T та 100Base-T в одній мережі (див. Д.6.1).

Робота мережі 100Base-T4. Мережа 100Base-T4, як уже зазначено, – це локальна мережа зіркової топології, яка використовує для передавання даних чотири пари провідників скрученої пари категорії 3, 4 або 5. Схема організації передавання показана на рис. 16.4.

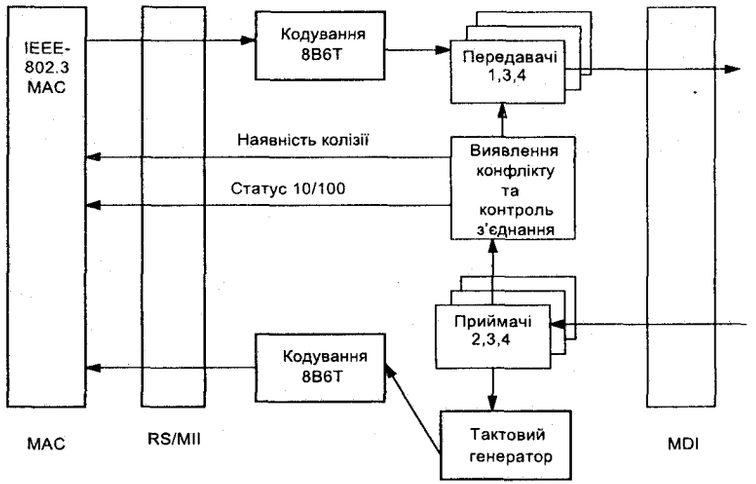


Рис. 16.4. Схема організації передавання 100Base-T4.

PCS кодує сигнали в трійковому коді, тобто кожен байт перетворюється на шість сигналів, кожний з яких має одне з трьох значень. Тому код позначають 8B6T. Розподіл дротів скрученої пари між сигналами показаний на рис. 16.5. У кожен момент часу передавання або приймання забезпечуть три пари дротів. Четверта пара призначена для виявлення конфліктів.

Швидкість передавання даних у мережі 100Base-T4 становить 100 Мбіт/с. Завдяки чому досягнута така швидкість?

- Використано три пари дротів, що дало змогу збільшити швидкість утричі;
- кодування 8B6T ще збільшило її в 2.67 раза;
- збільшено частоту з 20 до 25 МГц.

Усе це разом (3·2.67·1.25=10) і дало змогу досягти такої швидкості передавання.

Робота мережі 100Base-TX та 100Base-FX на фізичному рівні ґрунтується на специфікації **PMD** (Physical Media Dependent) ANSI, спочатку розроблених для волоконно-оптичних

мереж FDDI. Вона підтримує як скручену пару, так і оптичне волокно. PCS одержує обмежені стартовими та стоповими бітами байти даних зі швидкістю 100 Мбіт/с через MII в напівдуплексному режимі і перетворює їх у безперервний потік, який передається зі швидкістю 125 Мбіт/с у дуплексному режимі. Для цього використовується кодування 4B5B – до кожних чотирьох бітів додається п'ятий. Така схема кодування дає змогу зменшити рівень завад у каналі завдяки рівномірнішій 'густині' одиниць.

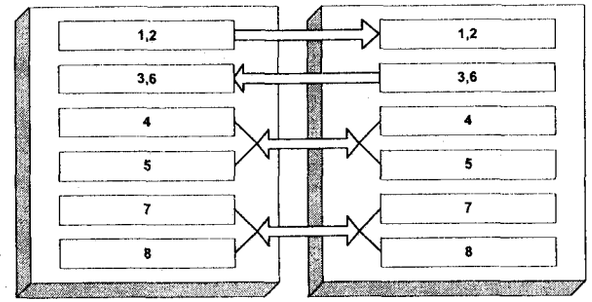


Рис. 16.5. Розподіл дротів скрученої пари між сигналами.

Приклади реалізації мереж Fast Ethernet. Розглянемо приклади використання технології Fast Ethernet на практиці з обладнанням фірми Allied Telesyn.

На рис. 16.6 показана структура мережі, в якій сегменти 10Base-T та 100Base-TX, реалізовані з використанням концентраторів AT-3624TR та CentreCOM MR912TX, об'єднані в єдину мережу простим двопортовим комутатором AT-MS203. Кожен порт цього комутатора має змогу автоматично самовизначати перепускну здатність приєднаного сегмента.

Подібні сегменти на рис. 16.7 об'єднані потужнішим комутатором CentreCOM RS710TX, який має як порти 10Base-T, так і порти 100Base-TX.

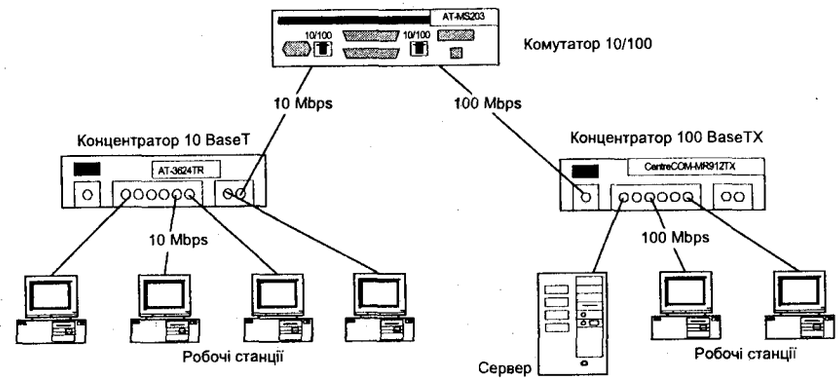


Рис. 16.6. Мережа технології Fast Ethernet.

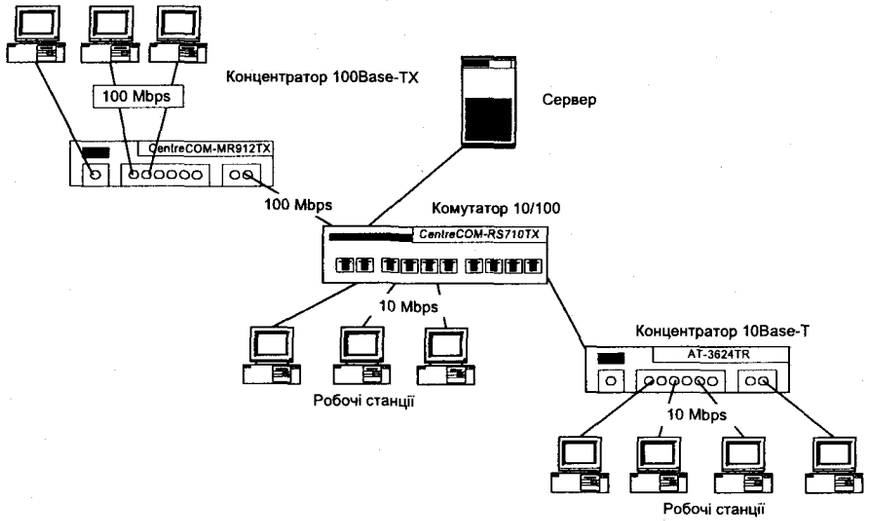


Рис. 16.7. Мережа технології Fast Ethernet.

16.3. Мережа 100VG-Anylan

Загальна характеристика, історія розробки, стандартизація. Локальна мережа специфікації 100VG-Anylan – це швидкісна (100 Мбіт/с) ЛМ зіркової топології, що має метод доступу з запитом пріоритетів. Мережа відповідає стандарту IEEE-802.12, прийнятому в червні 1995 р. У ній використовують скручену пару категорій 3, 4, 5, двожильний кабель з екранованими чи неекранованими скрученими парами або волоконно-оптичний кабель. Специфікацію 100VG-Anylan створено фірмами Hewlett-Packard та AT&T. Сьогодні власниками технології 100VG-Anylan є консорціум 100VG-Anylan Forum, до якого належать фірми Hewlett-Packard, AT&T, IBM, NTT, Asante та ін.

Позначення 'VG' у назві 100VG-Anylan означає, що можна використовувати скручену пару категорії 3 (Voice grade – та, що придатна для передавання мовлення). Слово 'Anylan' свідчить про можливість одночасного передавання кадрів різних типів мереж (802.3 Ethernet, 802.5 Token Ring).

Топологія, метод доступу та порядок роботи. Топологія мережі 100VG-Anylan – розподілена зірка. Метод доступу – з запитом пріоритетів (Demand Priority Access) (див. розділ 7) Кожен комутатор періодично опитує свої порти про наявність запиту від вузлів. Вузлом є сервер, робоча станція, маршрутизатор, міст, інший комутатор. Комутатор дає дозвіл певному вузлу передавати інформацію. Вузол тестує сполучення і передає інформацію комутатору, який

приймає кадр і передає його тільки в порт призначення. Це створює ще один рівень захисту даних (кадр не ретранслюється по всій мережі) та дає змогу зменшити інформаційні потоки в мережі (див. розділи 15, 19).

Кожен комутатор має один вхідний та кілька вихідних портів. Вхідний порт зарезервовано для зв'язку з комутатором верхнього рівня. До вихідних портів приєднують вузли мережі.

У мережі застосовують квартетне кодування. Послідовність бітів ділиться на групи по чотири для паралельного передавання всіма дротами скрученої пари. Дані передаються з частотою 30 МГц, схема кодування – 5B6B, тобто до кожних п'яти бітів додається один біт.

У ланцюжку з шести бітів велика ймовірність чергування двох логічних станів сигналу, потрібна для синхронізації приймача (див. розділ 3). Крім того, в цьому ланцюжку є збалансованість між 'одиницями' та 'нулями', що зменшує завади.

Обмеження та параметри продуктивності мережі. У мережі на шляху довільного кадру є не більше трьох послідовних комутаторів. Максимальний діаметр мережі – 2.5 км. Якщо в мережі використано волоконно-оптичні кабелі, то її довжина може досягати 4 км. Швидкість передавання даних залежить від передавального середовища. Зокрема, для неекранованої скрученої пари категорії 3 стандарт передбачає максимальну швидкість 100 Мбіт/с, а для скрученої пари категорії 5 – 150 Мбіт/с.

Мережа 100VG-Anylan невимоглива до типу та якості кабелю, порівняно дешева. У ній немає колізій. Тому при високих навантаженнях ступінь використання мережі досягає 95% перепускної здатності.

16.4. Мережа Gigabit Ethernet

Історія розробок. У листопаді 1993 р. була створена група для розробки специфікацій з підвищення швидкості передавання Ethernet до 100 Мбіт/с. У червні 1995 р. прийнято стандарт 100BaseT. Після підвищення швидкості доступу тісною для клієнтів стала магістраль. Тому групі з вивчення швидкісних технологій було доручено розглянути наступний рівень Ethernet. У липні 1996 р. інженерна група IEEE-802.3z почала розробку стандарту Ethernet зі швидкістю 1000 Мбіт/с. Стандарт Gigabit Ethernet IEEE-802.3z у частині, яка регламентує використання волоконно-оптичного кабелю, затверджено 25 червня 1998 р. Специфікація застосування скрученої пари виділена в окремий стандарт IEEE-802.3ab. Головна організація підтримки технології Gigabit Ethernet Alliance (GEA), що об'єднує понад 80 фірм.

Запозичення в технологіях. Fast Ethernet та Gigabit Ethernet є логічними розширеннями Ethernet. Однак обидві технології ґрунтуються на вирішеннях інших швидкісних технологій. Наприклад, фізичний рівень FDDI був запозичений та адаптований для Fast Ethernet. Аналогічно Gigabit Ethernet планує скористатися фізичним рівнем технології Fiber Channel, що дає змогу досягти швидкості передавання близько 800 Мбіт/с, однак завдяки збільшенню швидкості передавання сигналу до 1.25 Гбіт/с потенційна швидкість передавання становитиме 1 Гбіт/с.

Середовища передавання. Первинною специфікацією передбачено волоконно-оптичні кабелі Gigabit Ethernet (одно- та багатомодові) для магістралей, сполучення комутаторів, серверів. Довжина сегмента для багатомодового кабелю – 500 м, для одномодового – 2000 м. Залежно від місця застосування окремо визначені специфікації для коаксіальних кабелів, скрученої пари (настільна система).

Для передавання інформації волоконно-оптичним кабелем запропоновано два вирішення:

• *1000Base-SX.* Використання багатомодового волоконно-оптичного кабелю, передавання даних на максимальну відстань 275 м (або 550 м з застосуванням повторювача);

• *1000Base-LX.* Використання як багатомодового, так і одномодового волоконно-оптичного кабелю. В останньому випадку можна передавати дані на відстань до 5000 м.

Мідні кабелі можна застосувати в таких специфікаціях:

• *1000Base-CX.* Для передавання на відстань до 25 м застосовують коаксіальний кабель;

• *1000Base-T.* Використовують скручену пару категорій 6, 7. Максимальна відстань передавання – 100 м. Максимальний розмір домену колізій – 200 м.

Метод доступу та повторювачі. Аналогічно до старого Ethernet в Gigabit Ethernet використовують МДКН/ВК. Водночас збільшення швидкості передавання та частоти призводить до більшого загасання і меншої допустимої довжини сегмента. У Gigabit Ethernet цю проблему вирішують застосуванням повнодуплексних повторювачів, збільшенням міжкадрового проміжку з 64 (тривалість передавання 64 байт) до 512 байт. Запропоновано також збільшити мінімальну довжину пакета з 64 до 512 байт, а максимальну – з 1500 до 9000 байт. Порівняно з Fast Ethernet змінено схему кодування. Зокрема, 1000Base-T використовує п'ятирівневе кодування, а для зменшення впливу завад – восьмирівневий метод корекції помилок (4D Trellis Forward Error Correction). Сигнал має не два логічні рівні (0/1), а п'ять: –2, –1, 0, 1, 2. Інформаційні біти кодуються як –2/2 та –1/1, а 0 застосовують для контролю та корекції помилок.

Частота синхронізації сигналів 1000Base-T становить 125 МГц. Використовуються всі чотири пари дротів скрученої пари. Отже, швидкість передавання – 125·4=500 Мбод. Один імпульс передає 2 біти. Швидкість передавання даних – 500·2=1 Гбіт/с.

Проблеми міграції та типові застосування. Міграція відбувається поступово, з оглядом на наявні системи. Варіанти є такі:

а) канали між комутаторами та серверами (рис. 16.8);

б) модернізація каналів між комутаторами (рис. 16.9);

с) перехід до магістралі з комутатором або повторювачем Gigabit Ethernet (рис. 16.10).

На рис. 16.11 показано випадок застосування технології Gigabit Ethernet на обладнанні фірми Nbase. Два потужні комутатори, що підтримують як технології Fast Ethernet, так і Ethernet, сполучені каналом Gigabit Ethernet. До комутаторів приєднані як окремі робочі станції, так і цілі сегменти на базі концентратора 100Base-TX та комутатора 10/100 Base. Сервер приєднаний до комутатора повнодуплексним каналом Fast Ethernet з перепускною здатністю 200 Мбіт/с.

Продуктами Gigabit Ethernet є мережеві адаптери, комутатори, маршрутизатори, ретранслятори.

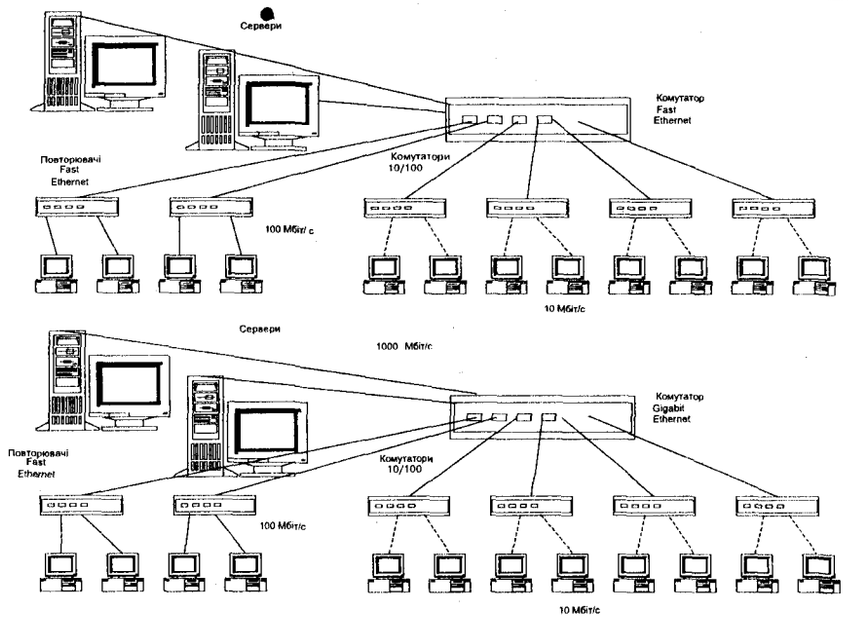


Рис. 16.8. Канали між комутатором та серверами.

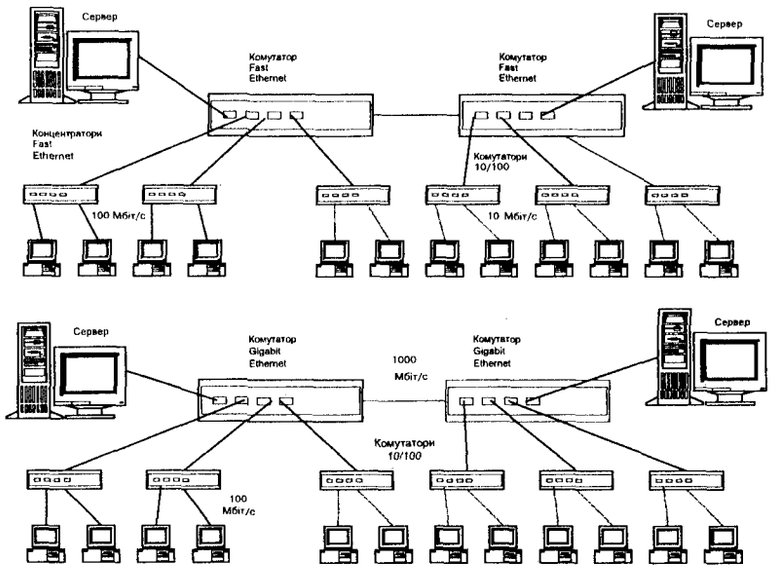


Рис. 16.9. Модернізація каналів між комутаторами.

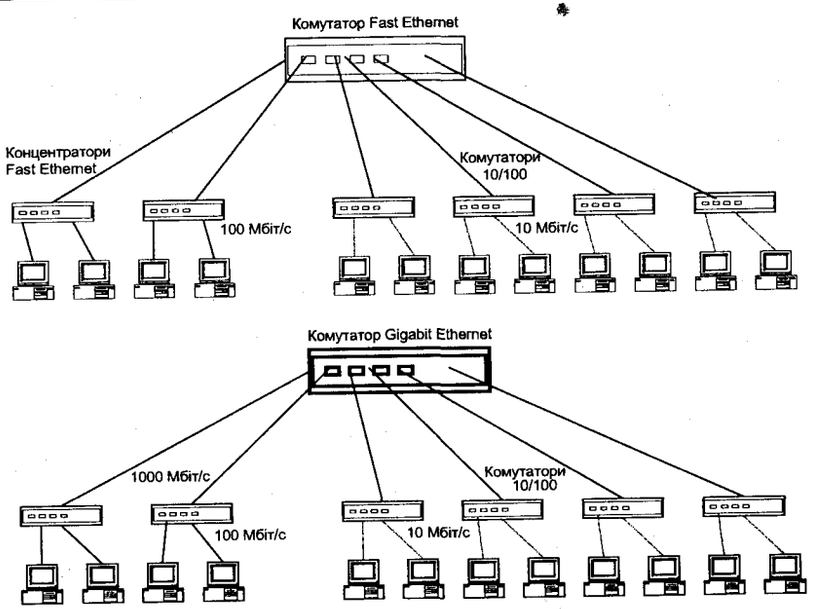


Рис. 16.10. Магістраль з комутатором Gigabit Ethernet.

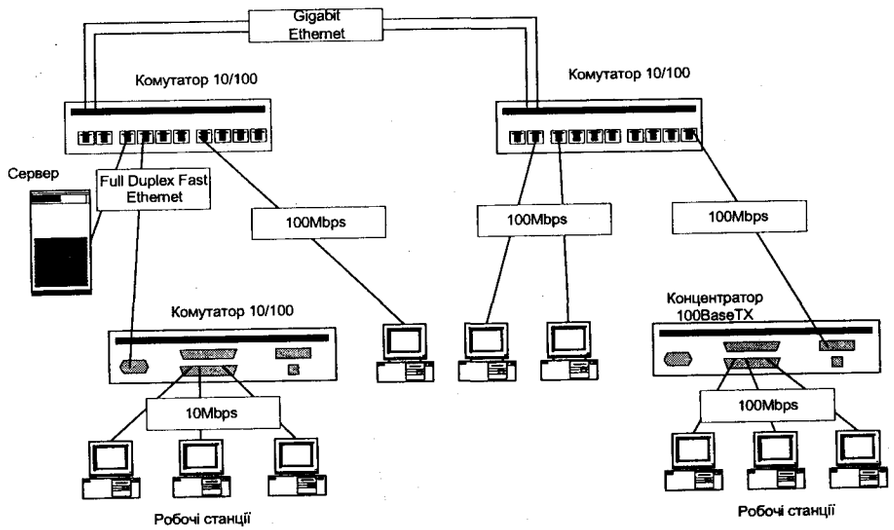


Рис. 16.11. Мережа Gigabit Ethernet на обладнанні Nbase.

Специфічним для технології Gigabit Ethernet є **буферний розподілювач** (buffered distributor). Це повнодуплексний багатопортовий пристрій, до якого приєднано два або більше каналів Gigabit Ethernet. Він не фільтрує кадри, однак для кожного порту має буфер. Буферний розподілювач є аналогом концентратора.

Бібліографія та джерела

1. *Ермолин А.А.* Стандарт 100Base-T: пора знакомиться // Сети. 1995. № 1.
2. *Карве А.* Ethernet – следующий рубеж // LAN. 1997. № 2.
3. *Карпенко А.* Дорога шириною в гигибайт // Чип. 1998. № 8.
4. *Кларк Э.* Gigabit Ethernet набирает скорость // LAN. 1998. № 3.
5. *Куин Л., Рассел Р.* Fast Ethernet. К.: BHV, 1998.
6. *Сатовский Б., Юрин В.* Gigabit Ethernet против ATM // Сети. 1997. № 1.
7. *Стром С.* Где и как применять Gigabit Ethernet // Сети. 1997. № 1.
8. Технологія 100VG-Anylan // Computerworld Kiev. 1996. 22 травня.
9. *Шатт С.* Мир компъютерных сетей. К.: BHV, 1996.

ЛОКАЛЬНА МЕРЕЖА TOKEN RING

Загальна характеристика та історія розвитку. Топологічна структура й алгоритм функціонування. Адресація, типи та структура кадрів. Функціональні ролі станцій. Процедури та алгоритми опрацювання помилок і збоїв. Нові версії та перспективи Token Ring.

17.1. Загальна характеристика та історія розвитку

Локальна мережа Token Ring – це мережа кільцевої топології з ретрансляцією та маркерним методом доступу. Її розробив у 60-х роках шведський інженер Олаф Содерблом. Запатентована в 1981 р. У 1985 р. прийнято стандарт IEEE-802.5 для мережі Token Ring зі швидкістю 4 Мбіт/с. Сьогодні є два варіанти цієї мережі – зі швидкостями передавання 4 та 16 Мбіт/с. Влітку 1998 р. прийнято стандарт IEEE-802.5t мережі Token Ring зі швидкістю 100 Мбіт/с. Розробляють варіант і на 1000 Мбіт/с. Власником та розробником мережі Token Ring є фірма IBM.

Порівняно з мережею Ethernet Token Ring посідає друге місце за використанням (наприклад, у 1993 р. у світі було випущено 8 млн адаптерів Ethernet, 2 млн Token Ring і 300 тис. Arcnet). Мережа Token Ring значно складніша, ніж Ethernet як технічно, так і алгоритмами та процедурами функціонування. Адаптери Token Ring у три-п'ять разів дорожчі, ніж адаптери Ethernet. Водночас Token Ring має і деякі переваги порівняно з Ethernet. Зокрема, вона ефективніше працює при великих навантаженнях (у цьому випадку Ethernet може використовувати до 30–40% від номінальної перепускної здатності, а Token Ring – 90%).

17.2. Топологічна структура й алгоритм функціонування

Топологічна структура Token Ring кільцева (рис. 17.1). Окремі станції приєднані через свої мережеві адаптери **NIC** (Network Interface Card). В адаптерній платі є кілька мікросхем, які виконують програмні функції керування передаванням даних у мережі. Комплект програм адаптерної плати називається *агентом*. Агент безпосередньо взаємодіє з протоколом сеансового рівня Netbios. Адаптерна плата приєднана до пристроїв багатостанційного доступу MAU (Multistation Access Unit) через спеціальний *абонентський кабель (lobe cable)*. Пристрої MAU мають по кілька роз'єднувачів для приєднання станцій і по два для приєднання у кільце. Якщо роз'єднувач станції порожній, то контакт у MAU замкнений і кільце замкнене. У випадку приєднання станції до MAU роз'єднувач розмикається і станція 'потрапляє' у кільце. MAU також сполучені між собою. Для передавання даних використовують чотирипроводову лінію (одне кільце резервне).

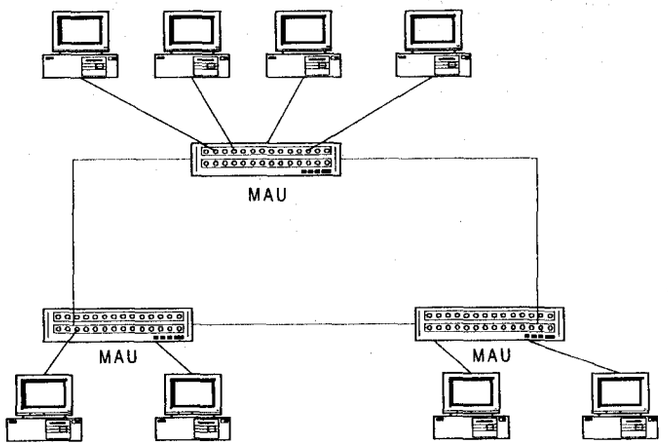


Рис. 17.1. Топологічна структура мережі.

У мережі Token Ring реалізовано маркерний метод доступу для мереж з ретрансляцією (див. розділ 7). Маркер – трибайтовий кадр, що циркулює кільцем. Станція, яка одержала маркер, усуває його з мережі і передає свій інформаційний кадр, який робить повне коло мережею та повертається до станції, яка його передавала. Ця станція усуває інформаційний кадр з мережі і передає маркер. Замість інформаційного LLC-кадру може передаватися службовий MAC-кадр.

17.3. Адресація, типи та структура кадрів

Є такі три типи адрес:

- індивідуальна – унікальна для кожної станції мережі;
- групова. Одна або кілька станцій об'єднані в групу. Їх адресують циркулярними повідомленнями для всіх членів групи;
- функціональна. У мережі є станції, які виконують конкретні передбачені для них функції. Деякі з них мають фіксовані адреси (сервер звітів про конфігурації, монітор помилок кільця, сервер параметрів кільця).

Кожна станція мережі Token Ring має індивідуальну адресу.

Для мережі Token Ring визначено три типи кадрів:

- кадр маркера;
- кадр даних;
- кадр послідовності аварійного завершення.

Розглянемо структуру цих кадрів.

Маркерний кадр має такі поля (рис. 17.2):

- *SD (Start Delimiter)* – заголовок.
- *AC (Access Control)* – поле керування.
- *ED (End Delemiter)* – кінцівка.

Рис. 17.2. Структура маркерного кадру.

Поле *SD* (рис. 17.3) складається з бітів *J*, *K*, що передаються з порушенням правил кодування Манчестерського коду (див. розділ 3).

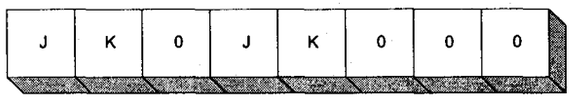


Рис. 17.3. Структура *SD*-поля.

У полі *AC* (рис. 17.4) *P* – біти пріоритету. У цьому полі записують біти поточного пріоритету. Тільки станція, яка має пріоритет, що дорівнює поточному, може використати маркер.

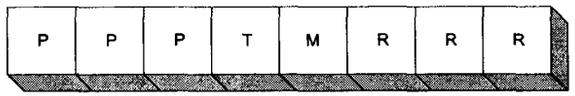


Рис. 17.4. Структура *AC*-поля.

Біти *R* резервні. Їх можна використовувати для оголошення станцією свого пріоритету для наступного одержання маркера.

Біт *T*=1, якщо кадр є кадром маркера.

Біт *M* є бітом монітора. Активний монітор надає цьому біту значення 1 для уникнення безмежної циркуляції маркера.

Поле *ED* (рис. 17.5) складається з бітів *J*, *K*, що передаються з порушенням правил кодування Манчестерського коду, *I* – біта-ознаки проміжного кадру, *E* – біта виявлення помилки.

Рис. 17.5. Структура *ED*-поля.

Кадр даних може бути керівним MAC-кадром або інформаційним LLC-кадром. Він має змінну довжину та може містити протокольний блок даних протоколу верхнього рівня. Його структура показана на рис. 17.6.

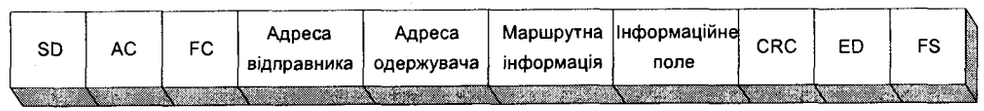


Рис. 17.6. Структура кадру даних.

Поля *SD*, *AC*, *ED* збігаються з аналогічними полями кадру маркера.

FC – поле керування кадром, визначає тип кадру (LLC або MAC) та ідентифікує MAC-кадр. Його структура зображена на рис. 17.7.

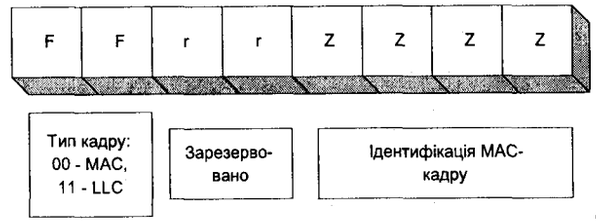


Рис. 17.7. Структура *FC*-поля.

Поле маршрутної інформації містить інформацію про маршрут передавання кадру, якщо цей кадр адресовано станції в іншому кільці. Це поле має змінну довжину (від 2 до 18 байт). Його опрацьовують мости та маршрутизатори.

FS – поле статусу кадру. Воно складається з таких бітів (рис. 17.8):

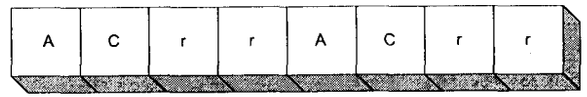


Рис. 17.8. Структура *FC*-поля: *A* – біти розпізнавання адреси, *C* – біти копіювання кадру.

17.4. Функціональні ролі станцій

Кожна зі станцій Token Ring може виконувати конкретні визначені функції; деякі з них можуть суміщатися.

Пасивний монітор (Standby Monitor (SM)) – це кільцева мережева станція загального призначення. Крім загального процесу передавання даних, SM стежить за наявністю в кільці

активного монітора. Якщо SM через деякий час не відшукують у мережі кадру *Active Monitor Present*, вони запускають процедуру оголошення маркера, в результаті виконання якої один з SM стає активним монітором.

Активний монітор (Active Monitor (AM)) є головним менеджером кільця. У кожний момент часу в кільці є тільки один AM. Він підтримує головний тактовий генератор мережі, періодично передає кадр *Active Monitor Present*, що дає змогу приєднувати та від'єднувати станції з кільця, перевіряє цілісність кільця та правильність передавання кадрів, у випадку збою запускає процедуру очищування кільця.

Сервер звітів про конфігурації (Configuration Report Server (CRS)). Якщо у складній мережі з кількох кілець керування мережею відбувається з використанням програми LAN Manager, то CRS збирає статистичну інформацію з кільця і надсилає її на консоль LAN Manager. CRS може змінювати та задавати параметри окремих робочих станцій та від'єднувати окремі станції з кільця за запитом консолі LAN Manager.

Сервер параметрів кільця (Ring Parameter Server(RPS)). У кожному окремому кільці одна зі станцій є RPS. Вона повідомляє новим станціям, які приєднуються до кільця, параметри (номер логічного кільця, номер версії ПЗ, значення таймера нерегулярних помилок), періодично передає на консоль LAN Manager зібрану інформацію про стан RPS та кільця.

Сервер помилок кільця (Ring Error Monitor (REM)) збирає інформацію про помилки. Як звичайно, для REM виділяють окремий комп'ютер, який аналізує регулярні та нерегулярні помилки. Якщо рівень нерегулярних помилок перевищено, REM намагається відшукати місце виникнення помилки (локалізувати домен несправності). Інформація про помилки передається на консоль LAN Manager.

Сервер моста (Local Bridge Server (LBS)). Якщо кілька кілець сполучені між собою мостом, то LBS виконує моніторинг даних, які передаються через міст. Статистичні дані передаються на консоль LAN Manager. LBS використовують і для збирання маршрутної інформації.

17.5. Процедури та алгоритми функціонування

Процедура вставляння в кільце запускається, якщо нова станція приєднується до кільця (MAU). Процедура складається з п'яти фаз.

• Перевірка якості зв'язку між NIC та MAU. Адаптерна плата передає MAC-кадр *Lobe Test*. Під час тестування фіксується частота бітових помилок у шлейфі між адаптерною платою та MAU. Якщо тестовий кадр без помилок одержано назад, то адаптерна плата передає на MAU сигнал приєднання.

• Аналіз наявності AM у кільці. Протягом деякого часу станція чекає, щоб прийняти один з трьох кадрів *Active Monitor Present*, *Reserve Monitor Present*, *Ring Purge*. Якщо кадр

надійшов, станція переходить до наступної фази. В іншому випадку запускається процедура *Оголошення маркера*.

• Перевірка унікальності адреси станції в кільці. Станція надсилає в кільце кадр *Duplicate Adress Test* і чекає на його повернення. Якщо кадр через визначений період часу не прийнято, станція виходить з кільця.

• Запускається процедура *Повідомлення сусіда*, під час якої станція визначає адресу свого безпосереднього сусіда (Upstream neighbor), який передає їй маркер. Станція повідомляє сусідові свою адресу.

• Ініціалізація станції. У кільце передається MAC-кадр *Request Initialisation*, адресований RPS. RPS у відповідь надсилає кадр *Initialize Ring Station*, де зазначено номер кільця, значення тайм-аутів для обліку нерегулярних помилок та інші параметри.

Після завершення цих фаз станція вважається приєднаною до кільця.

Режим нормального повторення. Кожна робоча станція аналізує всі кадри та маркери і ретранслює їх.

Процедура оголошення маркера полягає в тому, що SM намагаються одержати право відігравати роль AM. Процедура виконується у таких випадках:

• нова станція, що приєднується до кільця, не відшукує у ньому кадрів наявності AM;

• наявний AM протягом деякого часу не приймає кадрів;

• будь-який SM не відшукує протягом деякого часу AM або кадрів у кільці.

Під час виконання процедури станція може перебувати в одному з двох режимів: Claim Token Transmit (CTT) та Claim Token Repeat (CTR). Верх бере станція з найбільшою адресою. Вона стає AM.

Спочатку всі станції перебувають у режимі CTR. Станція, яка ініціює процедуру, надсилає у кільце кадр *Claim Token*, адресований собі. Після приймання цього кадру вона переходить у режим CTR та припиняє змагання. Кожна станція в режимі CTR порівнює свою адресу з адресою станції в кадрі *Claim Token*. Якщо її адреса більша, то вона переходить у режим CTT і передає свій кадр *Claim Token*. Процес відбувається в кільці доти, доки станція в режимі CTR тричі не прийме свій кадр *Claim Token*, після чого вона стає AM.

Процедура повідомлення сусіда. Важливим поняттям мережі Token Ring є адреса найближчого сусіда станції, від якого вона одержує маркер **NAUN** (Nearest Active Upstream Neighbour). Кожна станція може визначити адресу найближчого сусіда за допомогою процедури повідомлення сусіда. Для цього використовують два біти з поля статусу кадру: *A* – адреса розпізнана та *C* – кадр скопійовано.

• AM ініціює процес повідомлення сусіда, надсилаючи в кільце кадр *Active Monitor Present*. У цьому кадрі біти *A* та *C* становлять 0.

• Перший SM, який приймає цей кадр, визначає адресу попередньої станції за значенням поля *Адреса відправника*. Після тайм-ауту генерується MAC-кадр *Standby Monitor Present*. У цьому кадрі біти *A* та *C* також дорівнюють 0.

• Наступний SM, який приймає кадр *Standby Monitor Present*, діє аналогічно.

• Процес завершується, коли AM приймає кадр *Standby Monitor Present*.

Процедура очищування кільця полягає в тому, що кільце переходить у режим нормального повторення. Цей процес ініціюється АМ, якщо

- у кільці виявлені помилки (втрата маркера, збій у синхронізації);
- у полі керування *M*-біт дорівнює 1;
- кільце треба перевести в режим нормального повторення.

Пріоритетний доступ. Кожній робочій станції у кільці присвоєно пріоритет у керуванні маркером. Перші три біти маркера є бітами пріоритету. Станція, одержавши маркер, порівнює його пріоритет зі своїм і у випадку збігу має право на передавання. Якщо ж станція має менший пріоритет, ніж маркер, тоді вона просто ретранслює його. Останні три біти маркера станція використовує для заявки про свій пріоритет. Одержавши кадр, станція порівнює пріоритет, записаний у полі заявки пріоритету, зі своїм власним. Якщо вона має інформацію для передавання і її пріоритет більший від заявленого, то станція проставляє в полі заявки свій пріоритет. Отже, коли кадр повністю обійде кільце, в ньому буде записаний максимальний пріоритет станції, що потребує передавання.

Контроль кількості передавань полягає в тому, щоб кожен кадр зробив тільки один обхід кільця. Цю функцію виконує АМ з використанням біта моніторингу поля керування. Спочатку, під час передавання кадру станцією, біт моніторингу становить 0. АМ постійно аналізує його і, виявляючи 0, надає йому значення 1. Якщо ж АМ виявив кадр з бітом моніторингу, що дорівнює 1, то такий кадр знищується.

17.6. Опрацювання помилок

У процедурах керування мережі Token Ring розрізняють **нерегулярні** та **регулярні** помилки. Нерегулярна – це нестійка помилка, яка тимчасово порушує роботу кільця. Кожна станція має лічильник нерегулярних помилок, який фіксує кількість помилок за деякий період часу. Станція періодично подає для REM кадр *Report Soft Error* з повідомленням про частоту нерегулярних помилок і занулює значення лічильників помилок.

Якщо станція виявить, що в ній або в її NAUN виникає регулярна помилка, то вона адресує всім станціям MAC-кадр *Beacon*. REM, що прийняв цей кадр, подає на консоль LAN Manager попередження, яке фіксується в журналі збоїв.

Виявивши помилку знову, станція повторює передавання кадру *Beacon*, який ретранслюють усі станції. Після того, як NAUN станції прийме *Beacon* вісім разів, він тимчасово вилучає себе з кільця і виконує самотестування. Якщо під час тестування виявлені помилки, то NAUN повідомляє про це наступну станцію й остаточно вилучається з кільця. Станція приймає кадр *Beacon* і генерує кадр маркера. Мережа переходить у режим нормальної роботи.

Якщо NAUN успішно пройшов тестування, то сама станція тимчасово виходить з кільця і виконує самотестування. У випадку, коли один з тестів виявив помилку, станція вилучається з кільця остаточно. Після цього АМ запускає процедуру очищування кільця. Якщо сама станція під час тестування не виявила помилок, потрібне втручання оператора.

Інформація про виявлену несправність передається на консоль LAN Manager. У цьому випадку фіксується місце її виникнення (домен несправності) (сама станція, її NAUN або кабель між ними).

17.7. Нові версії мережі Token Ring

Поряд з класичним варіантом Token Ring, який працював зі швидкістю 4 Мбіт/с, розроблено модернізований варіант зі швидкістю 16 Мбіт/с. У чому ж головні відмінності цих мереж?

- Мережа на 16 Мбіт/с має більшу тактову частоту і смугу перепускання.
- Мережа на 16 Мбіт/с підтримує кадри більшої довжини. Якщо максимальний розмір кадру мережі 4 Мбіт/с був 4500 байт, то нової мережі – 18000 байт.
- У новій мережі для ефективнішого використання перепускної здатності введено механізм *випереджувального вивільнення маркера* (Early Token Release (ETR)). У мережі з ETR станція передає маркер відразу після передавання інформаційного кадру, не чекаючи, поки цей кадр обійде всі станції кільця.

Мережа Token Ring сьогодні уступає мережі Ethernet. Це зумовлено складністю технології Token Ring в експлуатації та адмініструванні, більшою вартістю обладнання. Незважаючи на появу комутованого TR, цей варіант мережі менш гнучкий і дорожчий, ніж комутований Ethernet. Невелика кількість портів у комутаторах Token Ring та невелика пропозиція на ринку зумовлюють суттєві проблеми в організації магістралей між мережами TR. Для цього доводиться застосовувати інші технології (FDDI або ATM). Головний напрям міграції – комутований Ethernet.

Бібліографія та джерела

1. *Нессер Дж.* Оптимизация и поиск неисправностей в сетях. К.: Диалектика, 1996.
2. *Толли К.* Token Ring: рынок призраков // Computerworld Россия. 1997. № 19(84).
3. *Хаусли Т.* Системы передачи и телеобработки данных. М.: Радио и связь, 1994.
4. *Шатт С.* Мир компьютерных сетей. К.: BHV, 1996.

ЛОКАЛЬНІ МЕРЕЖІ ARCNET, FDDI, FIBER CHANNEL, APPLETALK

Локальна мережа Arcnet: топологія, метод доступу. Мережа FDDI: топологія, структура кадрів, порівняння з Token Ring. Мережа Fiber Channel: головні параметри та сфера застосування. Мережева архітектура Appletalk: методи доступу, середовище передавання, головні протоколи та версії.

18.1. Локальна мережа Arcnet

Мережа Arcnet (Attached Resource Computer) – це маркерна локальна мережа зіркової або шинної топології, розроблена фірмою Datapoint ще на початку 70-х років. У ній використано маркерний метод доступу з формуванням логічного кільця та передавання спеціального кадру – маркера, який дає дозвіл на передавання. Специфікація мережі Arcnet описує не тільки метод доступу, але й електричні характеристики мережі. Вона наближена до стандарту IEEE-802.4, однак не повністю відповідає йому. Головна відмінність полягає в тому, що 8-розрядні адреси Arcnet не відповідають 48-розрядним адресам стандартів IEEE. Швидкість передавання інформації досягає 2.5 Мбіт/с. Довжина кадру становить 508 байт.

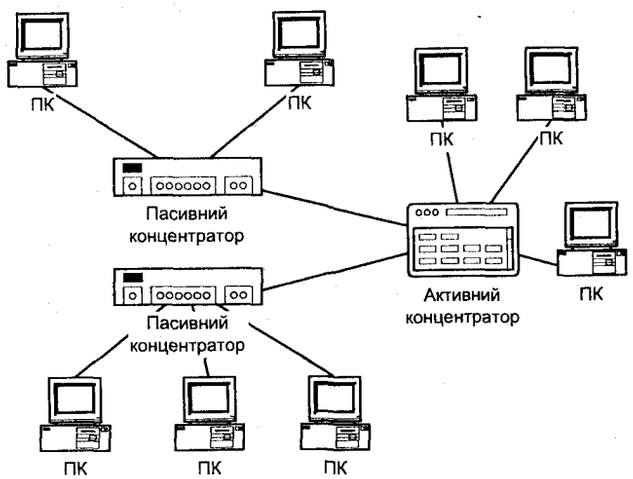


Рис. 18.1. Зіркова топологія мережі Arcnet.

У мережі Arcnet визначено дві топології: розподілена зірка та шина. Найпоширенішою є зіркова топологія (рис. 18.1). Робочі станції в такій мережі приєднані до концентраторів, які можуть бути **активними** (active hubs) та **пасивними** (passive hubs). Активні концентратори

підсилюють сигнал, мають зовнішнє живлення. До них можна приєднати до восьми станцій на відстані до 600 м. Пасивний концентратор тільки розгалужує сигнали. До нього можна приєднати лише чотири станції на відстані до 30 м.

Топологія шинної мережі Arcnet подібна до топології мережі Ethernet 10Base-2 (рис. 18.2). Станції приєднують через BNC Т-з'єднувачі. Вартість адаптерів мережі Arcnet залежить від топології мережі. Адаптери зіркової мережі значно дешевші, ніж адаптери Ethernet і втричі дешевші ніж адаптери Token Ring. Адаптери шинної мережі коштують майже стільки, скільки адаптери Ethernet. До однієї шини можна приєднати до восьми станцій.

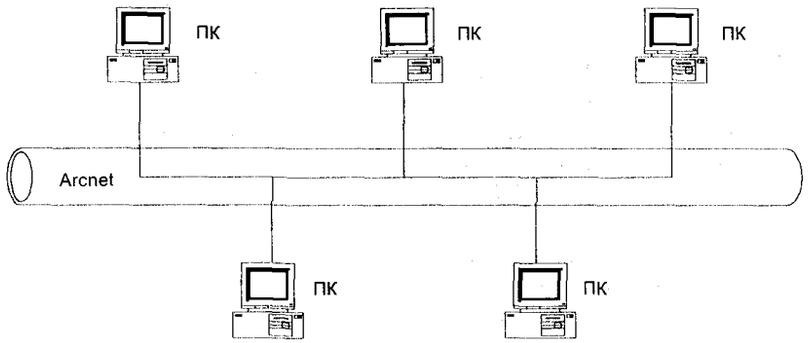


Рис. 18.2. Шинна структура Arcnet.

Мережа Arcnet не тільки найдешевша, але й має найгнучкішу та найпростішу у використанні технологію. Недоліком мережі можна вважати байт-орієнтований механізм взаємодії вузлів (спочатку запитується можливість передавання. Якщо приймач погоджується, відбувається передавання. Кожне передавання окремо підтверджується). Однак, незважаючи на появу мережі Arcnet Plus зі швидкістю передавання 20 Мбіт/с, збільшення максимального розміру кадру з 516 до 4224 байтів, підтримку 48-розрядної адресації та рівня керування доступом стандарту IEEE-802.2, її поступово витісняє мережа Ethernet.

18.2. Локальна мережа FDDI

Стандарт локальних мереж **FDDI** (Fiber Distributed Data Interface) належить до перспективних вирішень, що їх підтримують головні виробники комп'ютерної техніки. Його розробили спеціалісти групи X3T59.5 ANSI. З погляду топології мережа FDDI є подвійним волоконно-оптичним кільцем (друге кільце резервне). Швидкість передавання інформації у ній становить 100 Мбіт/с. Кожне кільце FDDI має довжину до 200 км. Окремі вузли мережі не можуть перебувати один від одного на відстані понад 2.5 км. Максимальна кількість станцій мережі – 1000. Мережі стандарту FDDI розглядають як перехідні між ЛМ та міськими мережами (MAN) стандарту DQDB.

Головним середовищем передавання FDDI є волоконно-оптичні кабелі. Водночас є розробки цієї мережі для роботи з мідним дротом – SDDI та CDDI. SDDI підтримує передавання даних екранованою скрученою парою (STP). Максимальна відстань передавання – 100 м. CDDI передбачає використання як екранованої, так і неекранованої скрученої пари.

FDDI максимально відповідає Token Ring, однак вона має і відмінності, зумовлені потребою збільшити швидкість передавання.

У мережі FDDI використано схему кодування 4B5B, яка кодує 4-бітові комбінації даних у 5-бітові комбінації світлових імпульсів так, що для передавання даних зі швидкістю 100 Мбіт/с реалізується швидкість передавання сигналів 125 Мбод.

На відміну від мережі Token Ring, у FDDI маркер передається відразу після передавання кадру станції, без очікування на повернення кадру кільцем. FDDI не використовує полів пріоритету та механізму резервування Token Ring. Натомість кожна станція класифікується, як асинхронна (що не ставить жорстких вимог до часу доступу) і синхронна (яка ставить такі вимоги).

Структура маркера мережі FDDI показана на рис. 18.3.

Преамбула	Початковий обмежувач	Контроль кадру	Кінцевий обмежувач	Статус кадру
8	1	1	1	
	SD	FC	ED	FS

Рис. 18.3. Структура маркера FDDI.

Зміст полів *SD*, *FC*, *ED*, *FS* відповідає змісту однойменних полів для мережі Token Ring. Структура інформаційного кадру зображена на рис. 18.4, а *FC*-поля на рис. 18.5.

Преамбула	SD	FC	DA	SA	INFO	FCS	ED	FS

Рис. 18.4. Структура інформаційного FDDI-кадру.

C	L	F	F	T	T	T	T

Клас кадру (асинхронний або синхронний)	Довжина адреси	Тип кадру (MAC/LLC)	Ідентифікація MAC-кадру

Рис. 18.5. Структура *FC*-поля.

Мережу FDDI найчастіше використовують для побудови магістральних мереж. Робочі станції, як звичайно, приєднані до портів концентраторів FDDI. Від'єднання будь-якої станції не спричинює зупинки в роботі мережі.

18.3. Волоконно-оптичний канал (Fiber Channel)

Fiber Channel – стандарт швидкісного передавання даних, який розробляють ANSI за підтримки IBM та HP. Він дає змогу передавати дані зі швидкостями понад 1 млрд біт/с волоконно-оптичним кабелем. Цей стандарт сумісний з наявними швидкісними інтерфейсами передавання даних HIPPI SCSI. HIPPI, наприклад, описує паралельний канал, що підтримує швидкості 800 або 1600 Мбіт/с для передавання даних на відстань до 25 м. Fiber Channel сьогодні застосовують головно для швидкісного передавання даних між головними та міні-ЕОМ. Налагодження сполучень у волоконно-оптичній комутованій технології (аналогічно, як через АТС) потребує багато часу (не менше 10 с). Тому Fiber Channel, який успішно використовують для зв'язку серверів, незадовільно працює в реальному масштабі часу. Технологія ATM забезпечує аналогічні параметри, однак з меншою вартістю адаптерів. Технологію Fiber Channel багато спеціалістів уважають тупиковою. Водночас технологічні напрацювання Fiber Channel використані у технології Gigabit Ethernet (див. розділ 16).

18.4. Архітектура локальних мереж Appletalk

Мережеву архітектуру **Appletalk** застосовують у локальних мережах комп'ютерів Macintosh. Як комп'ютери Macintosh, так і ця архітектура багато в чому несумісні з архітектурою мереж персональних комп'ютерів та інших мережевих архітектур. За багатьма технічними параметрами архітектура Appletalk значно поступається передовим мережевим технологіям.

Комп'ютери Macintosh випускають з вбудованим мережевим інтерфейсом LocalTalk. Кабельна система побудована на екранованій скрученій парі STP і дає змогу передавати дані зі швидкістю до 230.4 Кбіт/с відповідно до стандарту RS-422. Смуга перепускання кабелю розрахована на роботу тільки 25 користувачів.

Топологія мережі збігається із шинною топологією Ethernet. Проте замість методу доступу CSMA/CD тут використано його модифікацію – CSMA/CA (Collision Avoidance). Згідно з цим методом станція, що планує передавання кадру, прослуховує канал. Якщо канал вільний протягом 400 мс, станція чекає деякий випадковий інтервал часу і надсилає на станцію-одержувач кадр *Запит на передавання*. У випадку, коли одержувач відповідає кадром *Готовності до приймання*, станція-відправник надсилає кадр. Якщо відповіді не одержано, станція вважає, що була колізія, вичікує деякий випадковий час і знову робить спробу передавання.

Протокол доступу до каналу, що реалізує цей метод, називається **LLAP** (Local Talk Link Access Protocol). У першій версії мережі Phase1 адресні поля цього протоколу мали 8 бітів

(адреси 1–127 резервовані для станцій, а 128–254 – для серверів). Кадр мав змінну довжину і починався полем *прапорця*. Для гарантування унікальності прапорця використовували процедуру *бітстафінгу (bitstuffing)* (див. розділ 8).

В AppleTalk Phase1 окремі локальні мережі (максимум 32 станції) були об'єднані маршрутизатором або шлюзом у мережу. Максимальна кількість приєднаних станцій – 254. У новішій версії Phase2 на адресу виділено вже 24 біти, що дало змогу адресувати до 16 млн вузлів. Водночас мережеві вирішення Phase2 цілком несумісні з Phase1 та потребують повної заміни обладнання з великими витратами.

Для збільшення швидкості передавання інформації Apple випускає адаптери та драйвери доступу до мереж Ethernet та Token Ring – *EtherTalk* та *TokenTalk*.

Бібліографія та джерела

1. *Флинт Д.* Локальные сети ЭВМ: архитектура, принципы построения, реализация / Пер. с англ. М.: Финансы и статистика, 1986.
2. *Шатт С.* Мир компьютерных сетей. К.: BHV, 1996.

КОМУТАЦІЯ ЛОКАЛЬНИХ МЕРЕЖ. ВІРТУАЛЬНІ МЕРЕЖІ

Розділ 19

Техніко-економічні передумови та історія виникнення технології комутації локальних мереж. Головні принципи побудови та параметри комутаторів. Класифікація комутаторів. Віртуальні локальні мережі. Головні підходи до їхньої реалізації.

19.1. Технологія комутації локальних мереж

Техніко-економічні передумови та історія виникнення технології комутації локальних мереж. Одним із суттєвих недоліків популярної мережі Ethernet є недостатньо ефективне використання перепускної здатності каналу у випадку високого та середнього завантаження мережі. Крім того, значне зростання потреб користувачів щодо обсягів та швидкості передавання інформації спонукали інженерів розробити швидкісні й ефективні технології передавання даних на базі наявних Ethernet-технологій.

Одним з можливих варіантів вирішення цієї проблеми і стала технологія комутації локальних мереж як новий принцип організації самих локальних мереж та їхніх об'єднань (повнішу інформацію про засоби сполучення локальних мереж див. розділ 14). Історія розвитку комутаторів почалася з анонсування в 1990 р. фірмою Kalpana комутатора EtherSwitch, однак поширилася ця технологія тільки в 1993 р.

Мережа, що використовує технологію комутації ЛМ, побудована за топологією розподіленої зірки (рис. 19.1) У вузлах зірки розташовані комутатори. Вони, як і інші пристрої сполучення ЛМ (мости, маршрутизатори, шлюзи), аналізують та фільтрують інформаційний потік, у результаті чого частина інформаційного потоку мережі локалізується і не завантажує іншої частини мережі (рис. 19.2). Завдяки цьому можна досягти більшої перепускної здатності мережі.

Кожен комутатор має порти, до яких приєднані окремі станції або цілі сегменти мережі (див. рис. 19.1). На відміну від мостів, у комутаторах можна одночасно робити кілька сполучень між різними парами портів. Це дає змогу не тільки підвищити перепускну здатність, але й забезпечити більший захист інформації (дані не передаються через усю мережу) (рис. 19.3).

Крім того, у комутаторах можна виділити деяку частину перепусної здатності на окремий порт (наприклад, на порт, до якого приєднано сервер). Кожен комутатор є складним інтелектуальним пристроєм, яким звичайно керує протокол SNMP. Керування комутатором відбувається як через мережу, так і через виділений для цього роз'єднувач. У цілому мережа, побудована з використанням комутаторів за технологією комутації локальних мереж, є більш керованою ніж, наприклад, окремий сегмент 10Base-2.

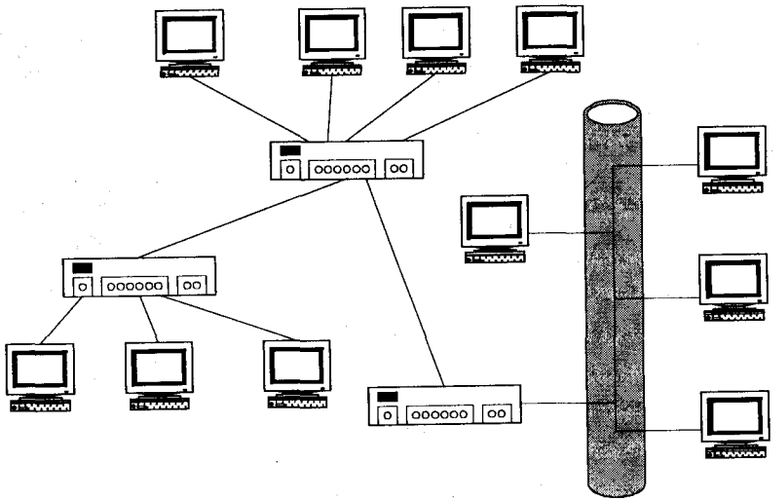


Рис. 19.1. Мережа з топологією розподіленої зірки.

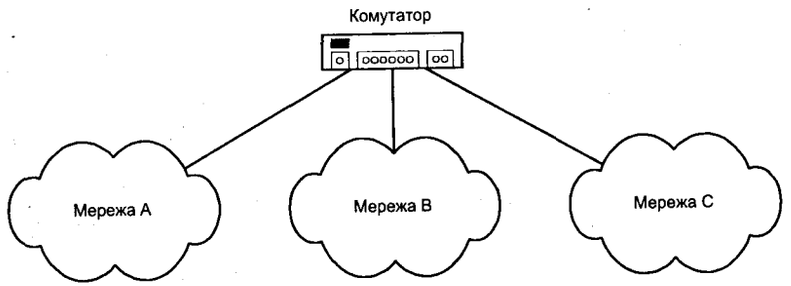


Рис. 19.2. Приєднання до комутатора.

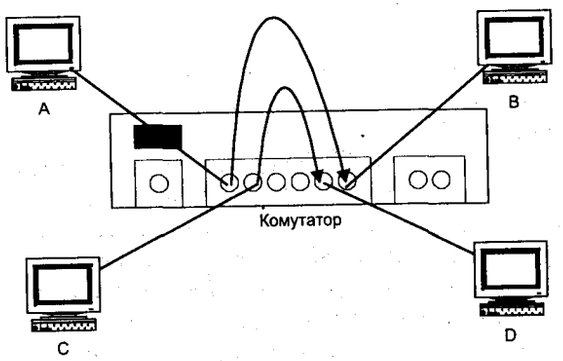


Рис. 19.3. Передавання інформації у комутаторі.

Зіркова топологія мережі та наявність керованих комутаторів роблять мережу стійкішою до збоїв, надійною в роботі. У такій мережі легше виконувати діагностику та шукати несправності.

Близько розташовані комутатори (і концентратори) можна сполучати в конфігурацію, що називається *стеком*. Комутаторні стеки використовують тоді, коли виникає потреба збільшити кількість портів. Застосування стеків – це найдешевший спосіб збільшити кількість приєднаних станцій та мереж.

Головні принципи побудови та параметри комутаторів. Для побудови комутаторів використовують один з таких двох принципів:

- **без буферизації** (cut-through);
- **з буферизацією** (store and forward).

У першому випадку комутатор починає передавати кадр, не очікуючи, поки завершиться його приймання, тобто відразу після визначення адрес призначення та відправника. Такий підхід дає змогу збільшити швидкість передавання пакетів, однак має й недоліки: зокрема, не можна передавати пакети між портами, які відрізняються швидкістю передавання (наприклад, між портами Fast Ethernet та Ethernet), неможливо перевіряти правильність передавання з використанням циклічного коду.

У випадку передавання з буферизацією комутатор повністю приймає кадр, аналізує його і тільки після цього спрямовує в порт призначення. Сьогодні переважають комутатори з буферизацією, що дає змогу використовувати в одному комутаторі порти різної швидкості. Комутацію без буферизації застосовують лише в дешевих комутаторах масштабу робочої групи.

Адресу відправника використовують для побудови таблиць адрес станцій, приєднаних до портів комутатора. Між окремими парами портів можна налагоджувати віртуальні сполучення, які існують протягом часу передавання кадру. Однак якщо кілька станцій передають інформацію в один порт, то вислідна перепускна здатність не перевищує перепускної здатності цього порту.

Показники продуктивності комутатора такі:

- продуктивність передавання з порту в порт (port-port forwarding bandwidth);
- загальна продуктивність (total forwarding bandwidth);
- затримка (latency).

Класифікація комутаторів. Є такі типи комутаторів:

- автономні комутатори робочих груп (не транслюють протоколи, не виділяють частину перепускної здатності для окремих пристроїв (серверів));
- комутатори, що забезпечують швидкісний зв'язок одного або кількох портів з сервером або магістральною мережею;
- комутатори відділу підприємства; їх використовують для взаємодії робочих груп; підтримують деревоподібну архітектуру зв'язків, фільтрування пакетів за певними ознаками;
- комутатори мережі підприємства; виконують функції диспетчеризації та маршрутизації; налагоджують віртуальні сполучення між мережевими сегментами.

Отже, комутатори – це альтернатива концентраторам та маршрутизаторам. Системи на базі маршрутизаторів не тільки коштують дорожче, ніж комутатори, але й мають більшу за-

тримку внаслідок аналізу мережевих таблиць для маршрутизації, виконання функцій протоколів мережевого рівня. Маршрутизатори доцільно використовувати в середніх та великих компаніях з територіально відділеними офісами. В інших системах ліпше застосовувати комутатори.

Вибір потрібного типу та марки комутатора – одна з ключових задач під час проектування комп'ютерної мережі. Як звичайно, виробники комутаторів пропонують серії комутаторів з різними функціональними можливостями й орієнтовані на вирішення певних задач.

19.2. Віртуальні локальні мережі

Історія виникнення віртуальних локальних мереж. Ідея побудови віртуальних локальних мереж виникла тоді, коли достатнього поширення набули об'єднання локальних мереж, а корпоративні мережі перетворилися на складні комплекси, які сполучали десятки окремих локальних мереж і тисячі комп'ютерів. Постала потреба об'єднати окремі невеликі групи станцій, які можуть бути розташовані далеко одна від одної, і надавати їм такий комунікаційний сервіс, який був би можливий за умови їх сполучення однією локальною мережею. Станціям такої **віртуальної мережі** (Virtual LAN (VLAN)) виділена певна частина перепускної здатності загальної мережі. Об'єднання у віртуальну локальну мережу динамічне, тобто окремі станції можуть входити та виходити з віртуальної локальної мережі без значних зусиль адміністратора.

Загалом концепція віртуальних мереж не обмежується створенням віртуальних локальних мереж. Вона має ширше завдання – зняти залежність між фізичною та логічною структурою мережі. Віртуальна логічна мережа, як деяке об'єднання користувачів або станцій, що має певні спільні вимоги до класу сервісу, повинна існувати незалежно від змін у фізичній структурі мережі, переміщення користувачів тощо. Найліпше реалізації цієї концепції відповідає АТМ-мережа. Вона надає клас сервісу за запитом, емулює локальні мережі.

Організація віртуальних мереж. У магістральному каналі мережі до службових повідомлень протоколу, який керує потоком, додається поле, що ідентифікує віртуальну ЛМ. За якими ж ознаками об'єднують станції у віртуальну ЛМ? Це можуть бути MAC-адреса, адреса локальної мережі, тип протоколу, а також комбінація цих ознак.

Є різні підходи до організації віртуальних ЛМ.

Найпростіший з них – **віртуальний сегмент**. Довільну кількість сегментів об'єднують в один віртуальний, що функціонує як замкнений домен трафіку. Після визначення такої мережі весь трафік між визначеними фізичними сегментами комутується зі швидкістю передавання фізичного середовища та з мінімальними затримками. Циркулярні повідомлення також обмежені віртуальним сегментом. Для керування трафіком між віртуальними сегментами застосовують мультипротокольні маршрутизатори (рис. 19.4).

У мережі протокольного стека TCP/IP віртуальні сегменти відповідають одній локальній мережі та забезпечують взаємодію мереж без посередництва маршрутизатора (у всіх станцій однакові адреси мереж).

У мережі стека SPX/IPX адреси локальних мереж сервер присвоює динамічно, під час реєстрації. Віртуальні ЛМ на базі віртуального сегмента не розпізнають типи протоколів мережевого рівня. Таке вирішення характеризується простотою та дешевістю.

Віртуальна ЛМ, побудована з підходом **віртуальної підмережі**, використовує комутатори, які працюють на мережевому рівні та розпізнають тип мережевого протоколу. Це дає змогу створювати віртуальні мережі одного типу протокольного стека (наприклад, TCP/IP). У таких мережах нема потреби в маршрутизаторах, їхні функції виконують комутатори.

Віртуальні мережі з таблицею MAC-адрес. Для кожної віртуальної мережі створюється своя таблиця MAC-адрес. ЛМ працює з будь-яким протоколом та адаптується до переміщення комп'ютерів.

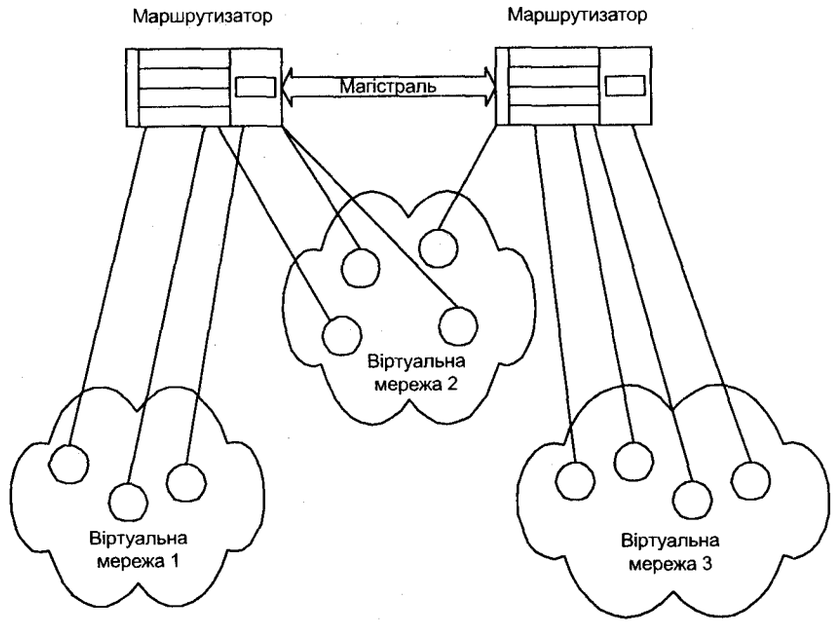


Рис. 19.4. Побудова віртуальних мереж.

Віртуальні ЛМ з автоконфігурацією не потребують деталізованих установок з боку адміністратора. Перший кадр у кожному сеансі надсилається на сервер маршрутизації для визначення, до якої віртуальної мережі належить станція. Такий сервер накопичує інформацію про всі станції та віртуальні мережі.

Стандарти віртуальних локальних мереж. Стандарти IEEE-802.1q та IEEE-802.1p дають змогу забезпечити взаємодію обладнання з різними реалізаціями VLAN у мережах Ethernet, обслуговування згідно з пріоритетами. Стандарти передбачають зміну структури кадру Ethernet з метою занесення інформації про пріоритети.

Стандарт IEEE-802.1q специфікує в кадрі Ethernet додаткове двобайтове поле, три біти якого кодують вісім рівнів пріоритету, 12 бітів використовують для запису належності до однієї з 4096 VLAN, один біт є позначкою кадрів інших мереж, які переносяться по Ethernet.

Стандарт IEEE-802.1p визначає алгоритм зміни порядку розташування кадрів у черзі відповідно до їхніх рівнів пріоритету. Можливе також використання інформації про класи та якість обслуговування.

Бібліографія та джерела

1. *Авдуевский А.* Такие реальные виртуальные сети // LAN Magazine. 1997. № 2.
2. *Кинг С.* К коммутируемому виртуальному будущему // Сети. 1995. № 5.

КАБЕЛЬНІ МЕРЕЖІ КМ. ТИПОВІ СТРУКТУРНІ ВИРІШЕННЯ

Розділ 20

Загальна характеристика та історія розвитку кабельних мереж. Прості та комбіновані кабельні мережі. Структуровані кабельні вирішення. Головні підсистеми. Типові структурні вирішення. Розподілена та централізована магістраль. Технологія DirecPC. Мережі кабельного телебачення.

20.1. Загальна характеристика та історія розвитку кабельних мереж ЛМ

Кабельна інфраструктура локальної мережі є однією з головних її елементів. На думку фахівців, власне помилки у кабельних з'єднаннях найчастіше є причиною збоїв у роботі мережі. Кабельні мережі розвивалися у напрямі від простих мереж шинної або кільцевої структури до комбінованих, а сьогодні логічно завершені в концепції структурованої кабельної системи. Є два підходи до цієї проблеми. Комп'ютерні фірми в розробках застосовують з'єднання комп'ютерів один з одним, поступово нарощуючи мережу. Комунікаційні фірми використовують кабельні телефонні мережі, які вже давно діють і мають складну розгалужену структуру, кроспанелі, розетки та ін.

Сьогодні актуальними є обидві тенденції, які мають суттєві переваги та недоліки. Прості мережі прокладають швидше, вони дешевші; розвиваються 'еволюційним' шляхом і не потребують значних капітальних витрат. Однак такі мережі складні в експлуатації та модернізації. Структуровані кабельні системи значно дорожчі, однак придатні значно довше (до 15 років, тоді як прості кабельні мережі доводиться замінювати вже після п'яти-восьми років експлуатації).

Кожен із варіантів кабельних мереж має свої обмеження, описані у специфікаціях протоколів та зумовлені технічними обмеженнями.

20.2. Прості кабельні мережі

Розглянемо прості кабельні мережі на прикладі мереж Ethernet. Головні варіанти специфікації Ethernet (10Base-5 та 10Base-2) мають обмеження щодо довжини з'єднань та кількості приєднаних пристроїв.

10Base-5. Швидкість передавання становить 10 Мбіт/с. Трансивери закріплені безпосередньо на кабелі роз'єднувачем з проколюванням ізоляції. Сегмент мережі має довжину до 500 м та максимально до 100 трансиверів. У мережу можна приєднати до п'яти сегментів,

отже, максимальна довжина кабелю між двома станціями становить 2500 м, а кількість повторювачів між довільними станціями – не більше чотирьох. Максимальна кількість станцій у мережі – 1024. Максимальна відстань між станцією і трансивером – 50 м (рис. 20.1).

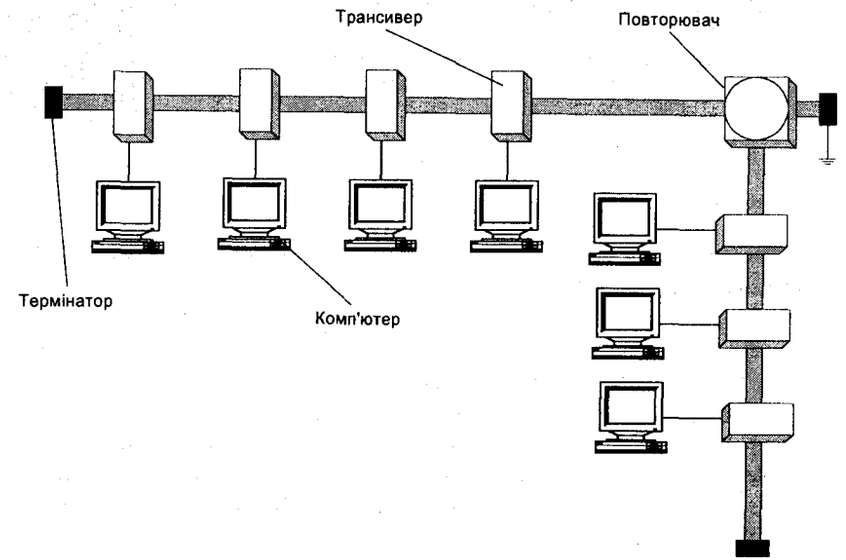


Рис. 20.1. Мережа 10Base-5.

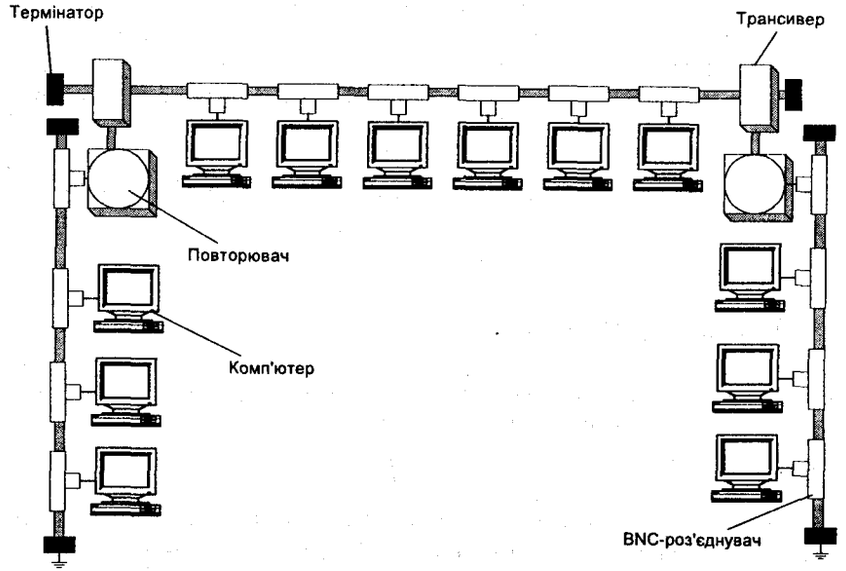


Рис. 20.2. Мережа 10Base-2.

10Base-2. Швидкість передавання становить 10 Мбіт/с. Станції мережі приєднані до кабелю через BNC-роз'єднувачі. Сегмент мережі має довжину до 185 м та максимально до 30 трансиверів. У мережі може бути до п'яти сегментів, отже, максимальна довжина кабелю між двома станціями – 925 м, а кількість повторювачів між довільними станціями – не більше чотирьох. У мережі також може бути до трьох сегментів, з'єднаних двома лініями завдовжки до 185 м кожна і без станцій. Максимальна кількість станцій у мережі – 150 (рис. 20.2).

10Base-T. Мережа Ethernet на скрученій парі побудована з використанням неекранованої (екранованої, фольгованої) скрученої пари. Вона має топологію розподіленої зірки і застосовує концентратори (рис. 20.3). Кількість станцій, які можна приєднати до мережі, залежить від кількості портів у концентраторах. Кількість портів можна збільшити побудувавши концентраторні стеки. Відстань між станцією та концентратором – не більше 100 м. Між будь-якою парою станцій не може бути більше п'яти сегментів та чотирьох повторювальних секцій. Сегментом уважають приєднання станції до концентратора та міжконцентраторні з'єднання.

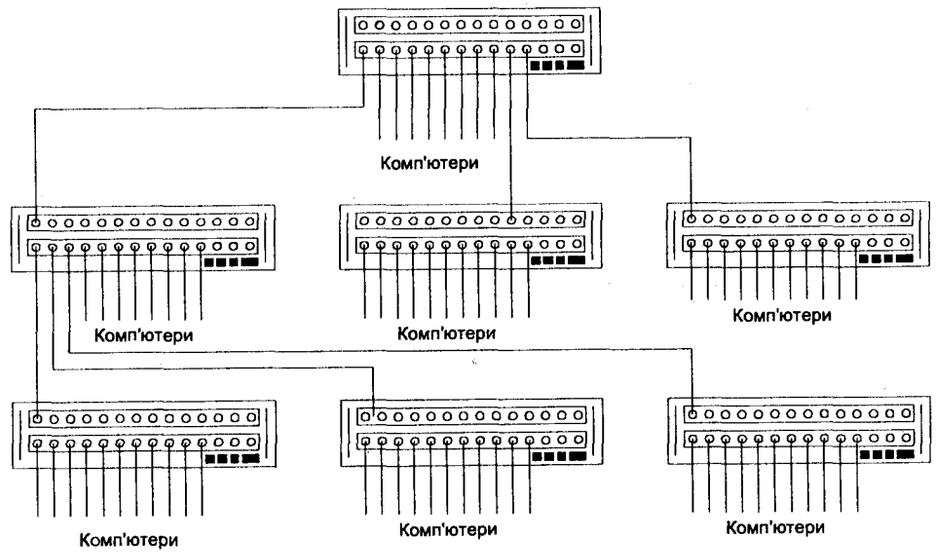


Рис. 20.3. Мережа 10Base-T.

З'єднання зіркової топології надійніші, прості в експлуатації, сумісні з сучасними технологіями Fast Ethernet та Gigabit Ethernet.

20.3. Комбіновані кабельні мережі

Комбіновані кабельні мережі застосовують, якщо потрібно частину мережі розмістити на більшій відстані, ніж дають змогу обмеження простих кабельних мереж. Розглянемо приклад комбінованої мережі з використанням скрученої пари та тонкого Ethernet (рис. 20.4). Сегмент 'тонкого' Ethernet приєднано через спеціальні AUI-роз'єднувачі концентраторів за допомогою кабелю зовнішнього доступу. На рис. 20.4 п'ятикутниками позначені та пронумеровані повторювальні секції, а квадратами – сегменти. Повторювальними секціями вважають як концентратори, так і повторювачі.

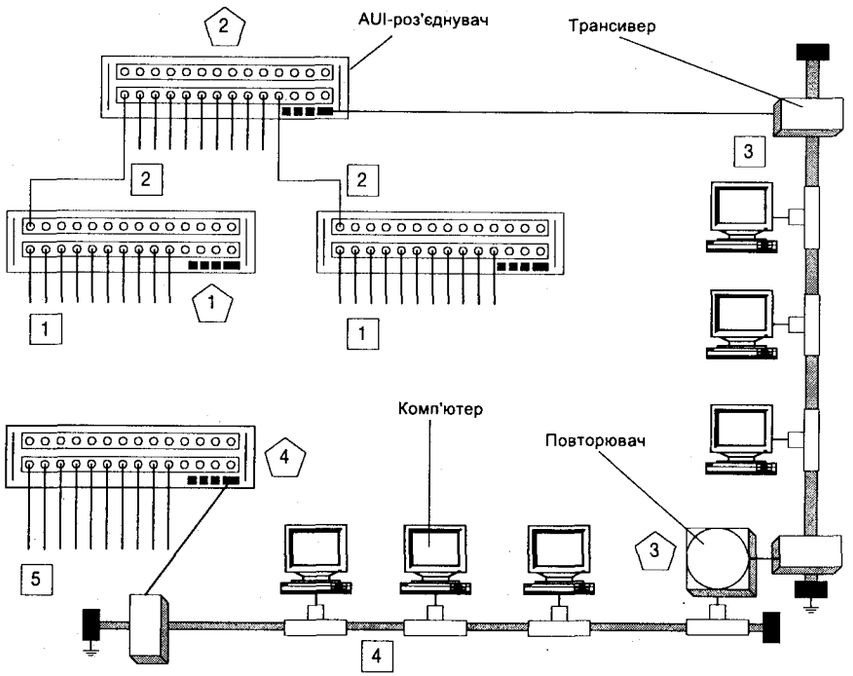


Рис. 20.4. Комбінована мережа.

Сегментами вважають кабельні з'єднання між станцією і концентратором, між концентраторами, між повторювачами, сегменти тонкого Ethernet. Максимальна кількість сегментів – п'ять, повторювальних секцій між довільною парою станцій – чотири.

Інколи структурні обмеження Ethernet подають у вигляді ***'правила 5-4-3'****: у мережі Ethernet може бути не більше п'яти сегментів, чотирьох повторювачів, однак тільки до трьох сегментів можуть бути приєднані клієнтські станції.*

20.4. Структуровані кабельні вирішення

У середині великого офісного будинку, як звичайно, монтують структуровану кабельну систему (рис. 20.5), яка складається з таких підсистем:

- вертикальної;
- підсистеми керування;
- горизонтальної;
- підсистеми робочого місця.

Вертикальна підсистема – це швидкісна міжповерхова магістраль. Її головно будують з використанням волоконно-оптичного кабелю або скрученої пари. Нею можна передавати дані зі швидкістю 100 або 1000 Мбіт/с. Для побудови застосовують мережі FDDI, комутований Fast-Ethernet, Gigabit Etgernet та ін.

Підсистему керування монтують на кожному поверсі. Вона складається з комутатора (або інших активних пристроїв) та комутаційної панелі. З використанням підсистеми керування адміністратор мережі перекомутовує окремі порти комутатора та розетки на поверсі. Комутатор та комутаційна (крос) панель розміщені в окремій шафі.

Горизонтальна підсистема – це кабельна мережа між комутаційною панеллю та підсистемою робочого місця. Для неї найчастіше застосовують скручену пару. Горизонтальну поверхову кабельну мережу монтують у спеціальних пластикових коритцях.

Підсистема робочого місця складається з розеток RJ-45 та *шнурів (patchcord)*, якими приєднані комп'ютери.

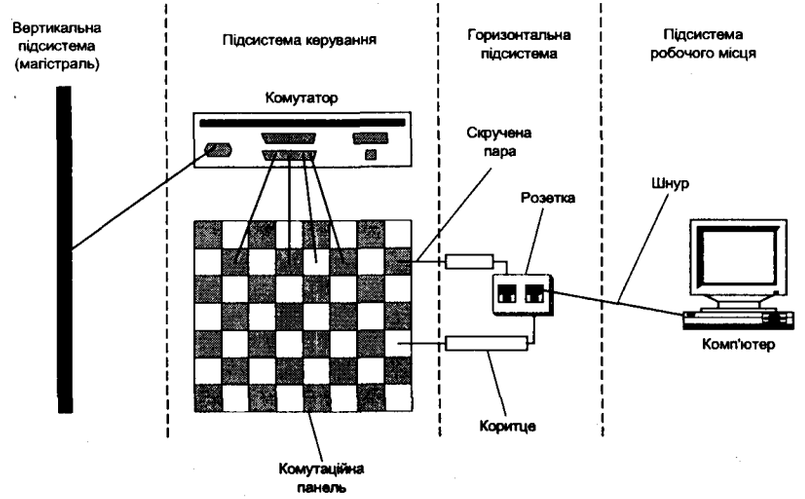


Рис. 20.5. Структурована кабельна система.

Структурована кабельна система, незважаючи на великі капітальні затрати, гнучкіша в експлуатації. Вона дає змогу однією і тією ж кабельною системою передавати інформацію різного типу: телефонні сигнали, дані, відеоінформацію охоронних систем тощо. Термін служби структурованої кабельної системи 10–15 років, що значно перевищує термін служби простих та комбінованих мереж. Структуровану кабельну систему прокладають, як звичайно, під час будівництва будинку офісу, її вартість закладена в капітальних витратах на будівництво. Простіші кабельні вирішення допускають поступове розширення і вкладання коштів. Водночас структурована система є єдиним правильним вирішенням у випадку побудови великих мереж з десятками серверів та кількома сотнями робочих станцій.

Прості кабельні мережі можуть прокладати спеціалісти середньої кваліфікації, в тому числі і представники фірми-замовника. Створити структуровану кабельну систему набагато складніше, це повинні виконувати представники спеціалізованої фірми. Під час побудови такої системи всі її компоненти (кабелі, комутатори, панелі, розетки, шнури тощо) й уся система повинні пройти сертифікацію на відповідність певній категорії або класу (наприклад, категорії 5, класу D). На ринку закінчені структуровані кабельні вирішення пропонують фірми MOD-TAP, Reichle&De-Massari (Freenet), AT&T (SYSTIMAX), Panduit (PANNET), Northen Telecom (IBDN) та ін.

20.5. Типові структурні вирішення

На ринку мереж сьогодні переважають декілька 'стандартних' мережевих архітектур. Пояснюють архітектури за допомогою графічних схем. Для позначення окремих типів активних пристроїв на схемах є система умовних позначень (рис. 20.6).

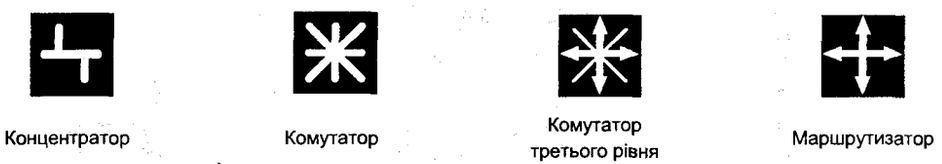


Рис. 20.6. Умовні позначення активних пристроїв мережі.

Розподілена мережева магістраль (distributed backbone) – одна з найперших мережевих технологій. В її основі є такий принцип: на кожному поверсі встановлено концентратор, який збирає весь трафік. Сполучення між поверхами налагоджують через маршрутизатори або за технологією локальних мереж чи з використанням FDDI (рис. 20.7). У такій мережі кожен сегмент – це окрема підмережа. Під час передавання даних між сегментами інформація проходить через маршрутизатори (додаткова затримка). Вартість такої мережі велика (багато маршрутизаторів), однак і велика надійність.

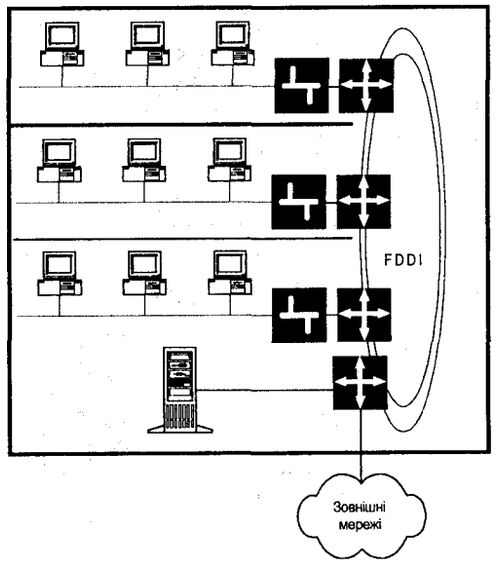


Рис. 20.7. Розподілена мережева магістраль.

Централізована мережева магістраль. Архітектура *Collapsed Backbone* виконана на основі базі центрального потужного маршрутизатора або комутатора. Її використовують для побудови мережі одного будинку (рис. 20.8). Центром магістралі можуть бути і концентратори, і маршрутизатори, і комутатори. Кожне з цих вирішень має відповідні обмеження. Зосередження магістралі в одному пункті створює зручну архітектуру для керування. Вартість такої мережі менша, зменшено затримки завдяки меншій кількості маршрутизаторів.

Для більшої гнучкості у центрі магістралі можна розмістити конфігурований комутатор. Це дасть змогу об'єднувати сегменти на різних поверхах в окремі підмережі, виділити окремий серверний канал, призначати та перепризначати сервери до окремих сегментів.

Така архітектура непридатна для з'єднань між будинками (навіть якщо вони розташовані близько).

Гібридні міжмережеві з'єднання (hybrid backbones). Кабельні з'єднання з кількох будинків зводити на один центральний пристрій складно. У цих випадках рекомендують гібридну мережеву архітектуру. Для магістралі можна використати технологію локальних мереж або FDDI, на рівні окремих будинків – централізовану магістраль, а для з'єднань між будинками – розподілену магістраль (campus backbone) (рис. 20.9).

Глобальна мережа. Найбільше архітектура глобальних мереж залежить від проблем економії. Якщо після створення локальної мережі нею можна користуватися майже безкоштовно, то за кожен канал глобальної мережі треба оплачувати провайдеру.

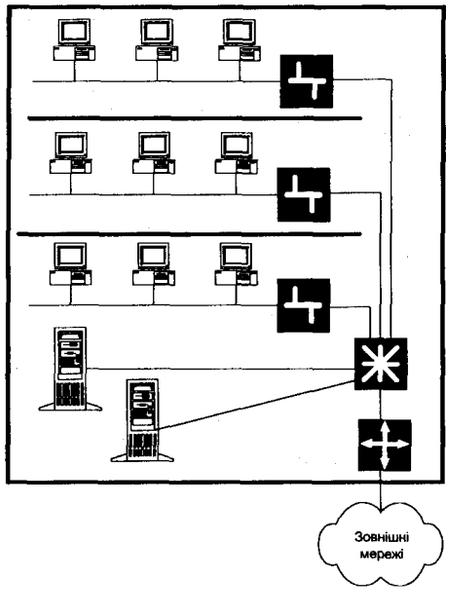


Рис. 20.8. Централізована мережева магістраль.

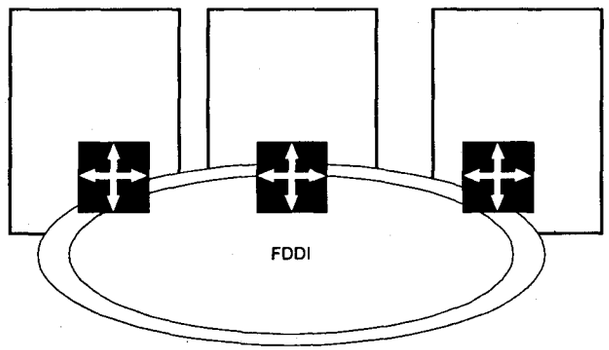


Рис. 20.9. Гібридне мережеве вирішення.

Вузлами глобальної мережі є маршрутизатори. Серед них виділяють головні вузли мережі (mesh backbone) з приєднаним до них 'кущем' маршрутизаторів для організації доступу (рис. 20.10). Як канали глобальної мережі (двопунктові) можна використовувати призначені канали різних типів та мереж.

Сучасність ставить нові вимоги щодо продуктивності мереж. Для збільшення перепускної здатності застосовують сегментацію та комутацію мереж, нові швидкісні технології.

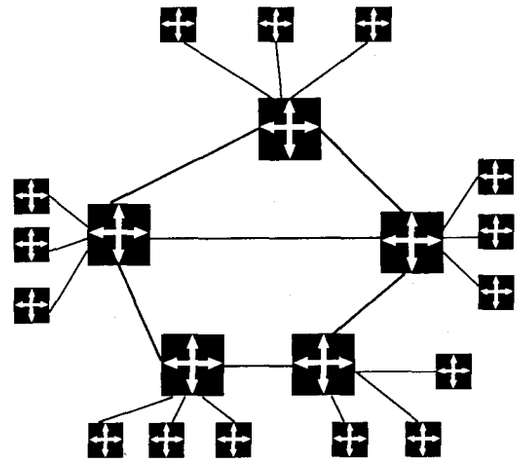


Рис. 20.10. Глобальні мережі.

Технології асиметричного передавання (DirecPC). Однією з технологій асиметричного передавання є гібридна технологія DirecPC (рис. 20.11). У цій технології користувач передає запит через звичайний комутований канал зв'язку і модем провайдеру послуг Internet. Зворотний шлях інформації інший: спеціальний центр супутникового зв'язку надсилає дані користувачу через супутник. Комп'ютер користувача обладнаний спеціальним адаптером та супутниковою приймальною антеною. Швидкість одержання даних значно перевищує швидкість надсилання запиту і становить 0.4–3.0 Мбіт/с. Подібний асиметричний порядок передавання виправданий, оскільки потік від сервера до користувача значно перевищує за інтенсивністю зворотний потік.

На комп'ютері користувача розміщений адаптер з відповідним драйвером, приєднаний до приймальної супутникової антени. Драйвер адаптера взаємодіє з ОС клієнтського комп'ютера як драйвер локальної мережі (специфікація NDIS). Водночас клієнтський комп'ютер через модем та комутовані телефонні канали приєднаний до Internet. Запит клієнта до будь-якого сервера Internet передається через модем. Драйвер адаптера в кожному IP-пакеті замінює зворотну адресу на адресу Операційного центру. Потім відбувається інкапсуляція цього пакета в інший IP-пакет, адресований Операційному центру та зі зворотною адресою комп'ютера-клієнта. Операційний центр одержує з такого подвійного пакета запакований первинний пакет, спрямовує його серверу й одержує відповідь, яку пересилає комп'ютеру клієнта супутниковим каналом. Отже, всі інформаційні потоки проходять через Операційний центр.

Технологію DirecPC розробила фірма Hughes Network Systems (HNS). Першу таку систему почали експлуатувати навесні 1995 р. Сьогодні пропонують три сервіси, що забезпечують таке:

• Turbo Internet – швидкісне низхідне передавання даних в Internet;

• Digital Packet Delivery – одночасне передавання великих файлів багатьом адресатам. Швидкість передавання може досягати 3 Мбіт/с;

• Multimedia – передавання телевізійних, навчальних та інших програм у реальному часі багатьом користувачам.

Подальшим удосконаленням DirecPC стала технологія **NetSat Direct**. На відміну від попередньої технології, тут є змога передавати запит безпосередньо через супутник з використанням мікрохвильового передавача (перепускна здатність 19.2 Кбіт/с). Нема потреби у висхідному модемному сполученні.

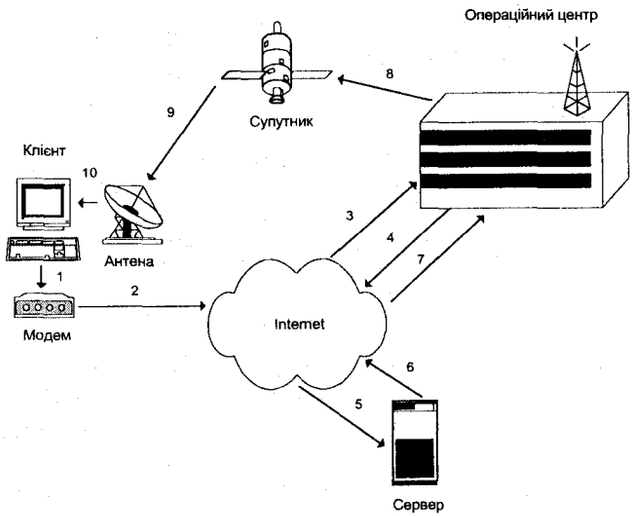


Рис. 20.11. Принципи функціонування DirecPC.

Технології мереж кабельного телебачення. Мережі кабельного телебачення створили з первинною метою розповсюджувати телевізійні програми. Найчастіше вони використовують аналогове передавання мідними коаксіальними кабелями.

Апаратна структура забезпечувала однонапрямлене передавання (від головного вузла до абонента). Зі збільшенням попиту на передавання даних та на послуги Internet виникла потреба надавати такі послуги абонентам з високою швидкістю та в обох напрямах. Задовольнити цю потребу, ще й за помірними цінами, дають змогу достатньо розгалужені мережі кабельного TV. Водночас сучасні кабельні мережі потребують деякої технічної перебудови для передавання даних.

Мережі кабельного TV мають деревоподібну структуру. Від головного вузла фірми – оператора послуг – розходяться коаксіальні кабелі. З метою поновлення аналогового сигналу та збільшення відстані передавання у мережу вмонтовані підсилювачі, які можуть бути однонапрямленими або двонапрямленими. Отже, мережі кабельного TV створюють багатопунктовий канал (єдине середовище передавання), не допускають комутації. Крім того, смуга перепускання

коаксіального кабелю недостатня для сучасних швидкісних технологій. Для передавання даних використовують спеціальні кабельні модеми.

Модернізація мереж кабельного TV полягає, головним чином, у заміні мідних коаксіальних кабелів волоконно-оптичними. Отже, мережі стають гібридними, волоконно-оптичними та коаксіальними (HFC). Смугу частот 750 МГц цих мереж звичайно поділяють на такі три діапазони:

• діапазон від 5 до 42 МГц застосовують для передавання у висхідному напрямі;

• діапазон 50–750 МГц використовують для передавання у низхідному напрямі;

• решта діапазону призначено для передавання сигналів телебачення.

Планується, що така кабельна інфраструктура та модеми дадуть змогу передавати інформацію у висхідному напрямі зі швидкістю 3 Мбіт/с, а у низхідному – до 30 Мбіт/с. Вислідна швидкість залежить від відстані передавання та наявного обладнання.

Багатопунктовий характер та сумісне середовище передавання створюють потенційні проблеми у випадку різкого зростання завантаженості мережі. Для реалізації двонапрямленого зв'язку треба повністю перейти на волоконно-оптичні кабелі та замінити однонапрямлені підсилювачі двонапрямленими.

Стандарти передавання даних у мережах кабельного TV тільки створюють. Головні оператори мереж кабельного TV об'єдналися в консорціум **Multimedia Cable Network System** (MCNS) та розробляють набір таких стандартів **DOCSIS** (Data Over Cable System Interface Specification). Окремі стандарти цього набору описують різні інтерфейси. Зокрема, інтерфейс CMCI визначає правила взаємодії апаратури користувача та кабельного модема, CMTS-NSI – правила взаємодії головного вузла магістральної мережі, серверів та центру керування. Інтерфейс CMTRI описує інтерфейс між апаратурою користувача та телефонною мережею, що дасть змогу використовувати мережу кабельного TV для надання телефонних послуг.

Бібліографія та джерела

1. *Акопов М.* СКС оптоволоконные и медные. Технологии удешевления монтажа // Сети и телекоммуникации. 1998. №4.
2. *Барабанов С, Коростелин А., Крюков С.* Компьютерные сети: вчера, сегодня, завтра //Компьютерпресс. 1997. № 2, 3.
3. *Гальперович Д.Я.* Открытым системам – открытые проводки // Открытые системы. 1995. № 3(11).
4. *Котас В.* Кабельные соединения по стандарту Ethernet // ReadMe. 1995. № 1.
5. *Ньюман Д.* Технологии доступа. Делайте ваши ставки // Сети и системы связи. 1997. № 11.
6. *Салтанов Д.А.* DirecPC доставит данные быстро! // Сети и системы связи. 1997. № 1.
7. Структурированные кабельные системы // Компьютерное обозрение. 1996. № 37(61).

АДМІНІСТРАТИВНА ПІДСИСТЕМА КМ

Рівні керування в комп'ютерній мережі. Призначення та функції адміністративної системи. Моніторинг і мережеметрія. Види та зміст звітів моніторингу. Планування робіт у мережі. Керування потоками і реконфігурування. Функції та призначення інформаційно-довідкової служби мережі. Електронна пошта.

21.1. Рівні керування в КМ

Виконання процедур керування в комп'ютерній мережі відбувається на чотирьох рівнях:

Стеження (Control) – це контроль нижнього рівня, виконується постійно на першому-четвертому рівнях протоколу розподілено багатьма незалежними процедурами керування.

Менеджмент (Management) – це функції керування сеансового та прикладного рівнів. До них належать налагодження та розірвання сеансу, одержання оплати за сеанси, рестарти.

Обслуговування (Maintenance) – передбачає підтримування мережі в робочому стані, ремонт, діагностування помилок з використанням спеціальних програм та технічних засобів діагностики.

Адміністрування (Administration) – це нагляд за функціонуванням мережі, її запуск та зупинка; забезпечення ефективності роботи.

З усіх прикладних процесів мережі виділяють один найважливіший – адміністративний, який і виконує функцію адміністрування. Користувач адміністративного процесу – *адміністратор* – має найбільші права щодо доступу до системи.

У великих мережах функції адміністрування можуть бути розподілені між багатьма адміністраторами. Зокрема, бувають адміністратори баз даних, захисту даних (security officers), архівування, електронної пошти (postmasters) та ін.

Головні завдання та групи функцій адміністративної підсистеми такі:
- моніторинг та мережеметрія;
- планування робіт у мережі;
- керування інформаційними потоками та реконфігурування мережі;
- інформаційно-довідкова служба;
- забезпечення безпеки даних, контроль за правильністю повноважень, розпізнавання;
- електронна пошта.

21.2. Моніторинг та мережеметрія

Моніторинг та **мережеметрія** – це безперервний контроль інформаційних та комунікаційних процесів у системі, збирання оперативних (моніторинг) та статистичних (мережеметрія) даних про якість функціонування мережі, використання її ресурсів тощо. Результати моніторингу попередньо опрацьовують та зберігають у спеціальних файлах моніторингу. На підставі цих даних за запитом адміністратора в будь-який час можна сформувати звіти. Є такі форми звітів:
- звіт про термінали (активність термінала, ім'я прикладної програми, яка працює на ньому, час активності);
- звіт про лінії (які станції зв'язані лінією, активність, статистика трафіку, відомості про повторення передавань, збої);
- звіт про прикладні програми (приєднання, статистика використання, з якими терміналами працює).

Статистичні дані про використання мережі обчислюють на підставі узагальнення оперативних. Мережеметрія дає змогу оцінити ступінь використання ресурсів мережі, ефективність її роботи.

Побічним результатом мережеметрії є генерування інформації для збирання оплати з користувачів: вона дає змогу зафіксувати, скільки кожен користувач працював у мережі, з якими програмами і на підставі цього вивести оплату. Крім того, моніторинг дає змогу стежити за діяльністю окремих користувачів з метою дотримання безпеки даних.

Моніторинг мережі виконується на багатьох рівнях мережі за допомогою спеціальних технічних засобів, протоколів, баз даних, служб. Проблематика моніторингу та діагностика мереж описані в розділі 22.

21.3. Планування робіт у мережі

Планування робіт у мережі передбачає збирання заяв від користувачів про їхні потреби в ресурсах мережі (передавання даних, віддалений доступ до інформаційних баз, програм, інформаційно-довідкових систем). Заяви користувачів аналізують, узгоджують і на їхній підставі виробляють план використання мережі.

21.4. Керування потоками та реконфігурування

У випадку приєднання до мережі нових комп'ютерів або виходу з ладу тих, що працюють, адміністративна система кожного разу змінює службові параметри керування відповідно до ситуації. Якщо вийшла з ладу якась ланка мережі, то адміністративна система може скерувати інформаційні потоки так, щоб обминути дефект.

21.5. Інформаційно-довідкова служба

Інформаційно-довідкова служба поширює в мережі інформацію про зміну структури об'єктів і ресурсів мережі, топології та послуг, повідомляє про появу нових програмних продуктів та послуг. Як звичайно, ця служба формує та підтримує довідник, у якому відображені:

- інформація про умови абонування, тарифи;
- мережевий абонентський довідник з адресами абонентів, їхніми ресурсами та послугами;
- види ресурсів (обчислювальні та інформаційні), що їх надають абонентам;
- інформація про загальнодоступні бази даних та їхні характеристики;
- правила поведінки абонентів щодо доступу та використання ресурсів.

Крім того, інформаційно-довідкова служба доводить інформацію за індивідуальними запитами або способом циркулярного повідомлення всіх абонентів чи групи. Для цього є спеціальний формат адреси. У сучасних мережах функції підтримки довідкової служби деякою мірою накладаються на функції ведення каталогу мережі (див. розділ 23), а також на функцію підтримки довідково-рекламної web-сторінки. Мережевий каталог містить довідкову інформацію, яку застосовують не тільки користувачі, але й операційні системи.

21.6. Електронна пошта

Повідомлення електронної пошти не є терміновими, тобто їх не обов'язково негайно передати абоненту. У комп'ютері користувача для електронної пошти відведено спеціальний каталог. Якщо абонент працює з ПК, то повідомлення записується на диск, не перериваючи роботи користувача з програмою; його можна прочитати згодом. Якщо ж комп'ютер користувача вимкнутий, то повідомлення зберігається на машині адміністратора і надходить на ПК користувача після ввімкнення комп'ютера в мережу. Користувача попереджають про надходження пошти.

Детальніше такі головні функції адміністративної підсистеми, як моніторинг, діагностування, служба каталогів, безпека даних, розглянуті у розділах 22–24.

Бібліографія та джерела

1. *Мартин Дж.* Системный анализ передачи данных: В 2 т. М.: Мир, 1995.
2. *Нессер Дж.* Оптимизация и поиск неисправностей в сетях. К.: Диалектика, 1996.
3. *Шатт С.* Мир компьютерных сетей. К.: BHV, 1996.

МОНІТОРИНГ, ДІАГНОСТИКА ТА КЕРУВАННЯ У КМ

Характеристика та класифікація засобів моніторингу. Діагностика кабельної системи. Використання рефлектометрів. Аналізатори протоколів та діагностика на рівні сегмента мережі. Головні функції та особливості роботи аналізатора протоколів. Розподілені системи керування мережею. Використання протоколу SNMP. База даних MIB. Протокол RMON. Аналіз та оптимізація КМ. Базовий рівень мережі. Головні завдання адміністратора та способи їх вирішення. Системи забезпечення якості обслуговування.

22.1. Загальна характеристика способів організації моніторингу в КМ

Завдання моніторингу (мережеметрії) та діагностики КМ тісно пов'язані. Їх виконують однаковими засобами одночасно. Детальний моніторинг системи потрібний для шукання причин несправностей чи незадовільного функціонування. Для зручності моніторинг доцільно вести на різних рівнях протоколу. Зокрема,

- на фізичному рівні досліджують параметри кабельної системи;
- на канальному та мережевому рівнях аналізують трафік, декодують та перехоплюють кадри і пакети;
- на верхніх рівнях протоколу вивчають взаємодію станцій з використанням конкретних протоколів та властивих їм параметрів;
- на рівні застосувань можливий аналіз взаємодії застосувань (наприклад, клієнта і сервера бази даних).

Адміністратора інформаційної системи передусім цікавлять параметри взаємодії застосувань. Однак причини неефективної роботи можуть бути зумовлені і роботою протоколів нижніх рівнів.

Крім протокольного рівня аналізу, системи моніторингу та керування відрізняються сферою дії (від окремого сегмента до великої глобальної мережі), рівнем інтелекту та сервісу (від простого перехоплення та відображення кадрів до складних експертних систем аналізу поведінки).

22.2. Діагностика на фізичному рівні

Найрозповсюдженішим пристроєм аналізу кабельної системи є **рефлектометр** (Time Domain Reflectometer (TDR)). Він виробляє та передає особливий сигнал у кабель і аналізує його відбиття. У кабелі можуть виникати такі несправності:

- обрив;
- коротке замикання;

• затиснення кабелю;
• погане навантаження;
• інше (згини, петлі тощо).

Рефлектометр аналізує луна-сигнал і порівнює його з сигнальними сигнатурами відомих несправностей, визначає можливий тип несправності та її місце.

Є також спеціальні пристрої діагностування кабелів, орієнтовані на конкретний тип мережі (наприклад, Ethernet або Token Ring). Вони виконують додаткові функції аналізу, що враховують особливості реалізації таких мереж.

22.3. Аналіз роботи сегмента з використанням аналізатора протоколів

Аналізатор протоколу – це програмно-апаратний блок, безпосередньо приєднаний до мережі. Він приймає весь інформаційний потік сегмента, декодує та інтерпретує його.

Головні операції, які виконує аналізатор – це *перехоплення*, *декодування*, *відображення даних*, *генерування тестових даних*. Адміністратор мережі використовує функції ініціалізації, фільтрування та відображення у різних форматах.

Фільтрування дає змогу виділити в загальному потоці пакети з певними ознаками. Сучасні аналізатори мають до кількох тисяч можливих умов фільтрування, за допомогою деяких можна комбінувати умови і навіть задавати їх вручну.

Ініціалізація допомагає пов'язати режими перехоплення та відображення з конкретними подіями. Визначена подія (наприклад, надходження кадру визначеного протоколу або певної довжини чи звертання до вказаного сервера) запускає перехоплення потоку.

Генерування тестових даних використовують для створення у мережі тестового потоку вказаного типу пакетів заданої інтенсивності.

22.4. Розподілені системи моніторингу та діагностування

Портативні аналізатори протоколів дають змогу простежити потік в одному окремому сегменті, до якого вони приєднані. Яким же чином виконати аналіз у складній, багатосегментній мережі? Можна перенести та приєднати аналізатор до іншого сегмента. Однак це потребує додаткових витрат та не описує однакового в часі стану мережі. Крім того, цей метод не можна застосовувати у великих корпоративних мережах, де окремі сегменти можуть бути розділені територіально на тисячі кілометрів. Використання технології комутації, крім очевидних переваг, спричинює й певні незручності аналізу потоку (аналізатор 'бачить' трафік тільки на одній з гілок комутатора). Тому для великих розподілених систем, крім аналізаторів, застосовують агенти моніторингу та аналізу, бази даних параметрів стандарту MIB, протоколи SNMP та RMON, розподілені системи моніторингу та аналізу.

Опишемо загальну структуру системи моніторингу (рис. 22.1). На нижньому рівні ієрархії є програмно-апаратні агенти, розподілені мережею. Це можуть бути окремі пристрої, блоки в комутаторах та маршрутизаторах, програми в комп'ютерах мережі. Агенти збирають та зберігають інформацію про свій сегмент і передають її так званій *платформі керування* – центральній програмі, що виконує всі функції аналізу та взаємодіє з користувачем. Платформа керування може містити програмні блоки – продукти інших виробників, або бути складовою частиною іншого застосування.

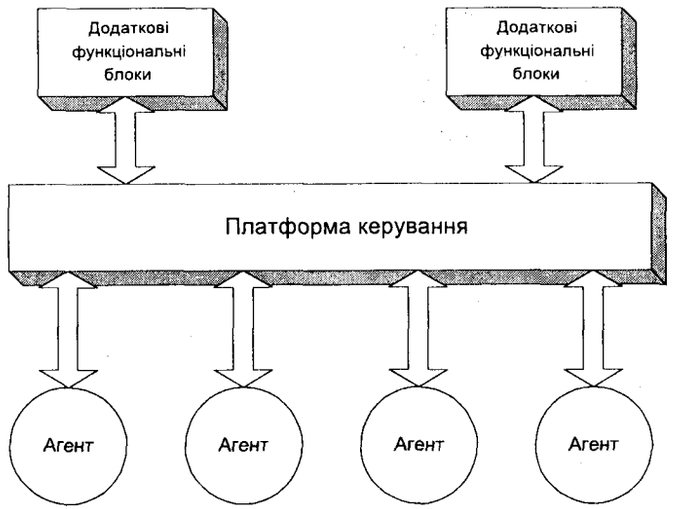


Рис. 22.1. Структура розподіленої системи керування мережею.

Агенти в розподілених системах керування функціонують та взаємодіють з платформою керування за допомогою протоколів SNMP або RMON. Більшість мережевих пристроїв сьогодні підтримує протокол керування SNMP та базу даних MIB (див. Д.22.1, Д.22.2, а також розділ 13). Недоліком SNMP є недостатня 'інтелектуальність', тобто агенти цього протоколу передають результати вимірювань за запитом, однак не узагальнюють та не опрацьовують локальні дані. Це перевантажує мережу зайвою інформацією. Подальшим розвитком SNMP став протокол RMON (див. Д.22.3). У ньому реалізовано деякі функції опрацювання та узагальнення інформації самим агентом. Завдяки цьому зменшується кількість службової інформації в мережі. Прикладом такої розподіленої системи керування є система фірми Network General – *Distributed Data Sniffer*. Вона не тільки збирає та узагальнює інформацію з окремих сегментів мережі, а й завдяки своїй експертній підсистемі генерує рекомендації для адміністратора мережі (див. Д.22.4).

22.5. Огляд платформ керування

Платформа керування – це центральна програма, яка збирає, опрацьовує та відображає дані аналізу й моніторингу, зібрані розподіленими агентами. Серед комерційних варіантів таких програм можна назвати *Spectrum Enterprise Manager* (Cabletron), *OpenView Network Node Manager* (Hewlett-Packard), *TIME 10 NetView* (IBM), *Domain Manager* (Sunsoft). Головні функції платформ керування такі:

- автоматичне визначення топології;
- стеження за мережевими подіями;
- керування мережевими пристроями з використанням SNMP, відображення їхнього стану, робота з базами MIB.

Автоматичне визначення топології потребує побудови дерева взаємопов'язаних маршрутизаторів. Для великих мереж це досить трудомістке завдання (потрібно близько доби) і дає неоднозначні результати. Тому в платформах керування передбачена можливість ручної корекції.

22.6. Аналіз та оптимізація комп'ютерних мереж

Використання аналізатора протоколу в окремому сегменті, а розподілених систем у складних багатосегментних мережах має на меті не тільки шукання несправностей, а й оптимізацію та налагодження параметрів мережевих пристроїв. Оптимізація мережі дає змогу використовувати її максимально ефективно, домогтися максимуму віддачі від наявної конфігурації апаратного та програмного забезпечення. Формалізованих методів оптимізації мережі нема. Сьогодні цей процес можна вважати мистецтвом – велике значення має інтуїція, досвід аналітика, його знання. Водночас можна виділити набір загальноприйнятих задач, що визначають базові функції.

Визначення базового рівня мережі (network baselining) – це періодичне вимірювання та реєстрування рівня функціонування мережі. Кожна мережа має визначений статичний рівень роботи (static baseline), який час від часу, в результаті роботи застосувань мережі, може змінюватися. Загалом статичний рівень визначає деякі усереднені за конкретний період значення параметрів навантаження та продуктивності мережі. Різка зміна базового рівня може бути спричинена несправністю.

Головні характеристики статичного рівня мережі такі:

- завантаження смуги перепускання всієї мережі та між окремими вузлами;
- склад протоколів;
- типи та рівні помилок;
- статистика та операції кадрів фізичного рівня та протоколів верхніх рівнів.

Базовий рівень у мережі визначають періодично й обов'язково документують у спеціальному журналі відображення параметрів мережі. Крім періодичних перевірок, базовий рівень визначають і у випадку різких змін у мережі, введення нового обладнання, застосування тощо.

Вимірювання часу реакції. Час реакції – це час, потрібний для одержання відповіді на конкретний запит чи подію. Різке збільшення часу реакції є ознакою несправностей у мережі. Для вимірювання цього часу використовують аналізатор протоколу та засоби моніторингу. Щоб визначити час реакції, потрібно простежити за всіма етапами формування відповіді на запит (*причина проблем може бути в довільній ланці шляху*). Одержані результати порівнюють з аналогічними результатами попередніх вимірювань.

Визначення ефективності мережевих застосувань. Адміністратор мережі повинен знати ступінь завантаження перепускної здатності мережі різними застосуваннями. Кожне застосування має стандарний час реакції у випадку звертання до мережі. Цей час залежить не тільки від параметрів мережі, а й від конфігурації самих застосувань, клієнтів та серверів. Деякі застосування можуть конфліктувати під час звертання до спільних ресурсів. Обов'язком адміністратора є підтримання нормованого часу реакції застосувань, їхня коректна конфігурація.

Визначення реальної перепускної здатності. Кожен пристрій, який приєднують до мережі, має зазначені у документації максимальні параметри продуктивності – швидкість передавання, кількість пакетів, які опрацьовує за секунду тощо. Адміністратор мережі повинен для кожного такого пристрою визначити реальні параметри перепускної здатності в різних режимах роботи. Для цього він виконує тестові вимірювання роботи пристрою в екстремальних умовах. Генерувати тестовий потік завантаження пристрою можна за допомогою аналізатора протоколів. Виміряну перепускну здатність пристрою порівнюють з паспортною та документують.

Визначення часу передавання файлу. Одним з найпопулярніших сервісів сучасних мереж є застосування файл-сервера для спільного використання файлів. У таких мережах доцільно вимірювати час передавання файлу визначеного розміру у випадку нормованого завантаження мережі.

22.7. Розподілені системи забезпечення якості обслуговування

У сучасних мережах передають одночасно потоки з різними вимогами до параметрів передавання. Це звичайні дані, відео та аудіоінформація, телефонні розмови, інформація керування та моделювання. Тому потрібно, зважаючи на наявне комунікаційне обладнання, забезпечити якісне передавання кожного типу потоку. Це зумовило появу нових систем мережевого керування, які оперують поняттям **якості обслуговування** (Quality of Service (QoS).

Якість обслуговування відображає здатність гетерогенної мережі надавати окремим інформаційним потокам більшу смугу перепускання, ніж іншим, що відображається у параметрах затримки передавання (delay), спотворення міжпакетних інтервалів (jitter), інтенсивності втрат пакетів та ін.

Сьогодні розрізняють три рівні забезпечення QoS:

- *за змогою* (Best Effort) – якість передавання не гарантована;

• *вибіркове обслуговування* (Soft QoS) – деяким потокам надано переваги; в середньому вони передаються швидше, з меншими втратами, ніж інші, однак конкретні параметри не гарантовані;

• *гарантовані послуги* (Hard QoS) для певних потоків забезпечено визначені параметри якості передавання.

Продуктом, що має на меті забезпечити QoS в гетерогенних мережах, є **Internetwork Operation System (IOS)** фірми **Cisco** – провідного виробника активного мережевого обладнання для різних типів мереж. Складовою частиною IOS є набір програм, методів та засобів, який має на меті забезпечити наскрізні параметри якості обслуговування в об'єднаннях різнотипних мереж (Ethernet, IEEE-802.1, Frame relay, ATM, SDH, послідовних каналах, сполученнях з головними ЕОМ IBM та ін.).

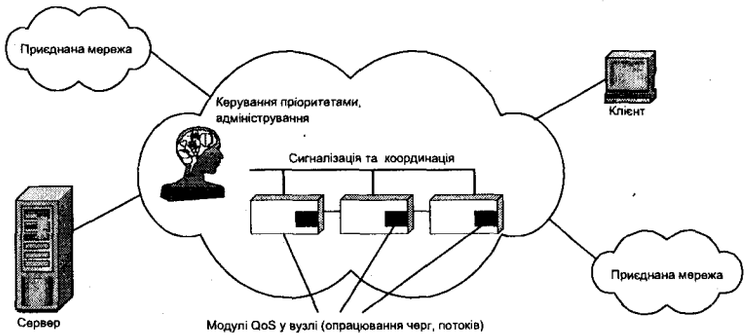


Рис. 22.2. Структура системи забезпечення якості передавання.

Архітектура QoS складається з таких частин (рис. 22.2):

• засоби забезпечення QoS в окремих мережевих пристроях (процедури опрацювання черг, керування потоком, диспетчеризації);

• методи та механізми координації діяльності пристроїв у мережі для забезпечення наскрізних параметрів якості передавання потоку;

• засоби та платформи керування для аналізу та керування наскрізними параметрами потоків для адміністратора мережі.

Детальніша інформація про IOS наведена в Д.22.5.

Бібліографія та джерела

1. *Крейнес А.* RMON переходит в наступление // Сети. 1996. № 6.
2. *Молостов В.И., Храмцов А.В.* Сетевые анализаторы //Сети. 1995. № 4.
3. *Нессер Дж.* Оптимизация и поиск неисправностей в сетях. К.: Диалектика, 1996.
4. *Шатт С.* Мир компьютерных сетей. К.: BHV. 1996.
5. *Штайнке С.* Рентгеновский снимок сети // LAN Magazine/RE. 1996. № 4.
6. Cisco IOS™ Software. Quality of Service Solutions. Cisco Systems white paper. 1999.

ДОДАТКИ ДО РОЗДІЛУ 22

Д.22.1. Протокол SNMP

SNMP (RFC-1157, 1215, 1187, 1089) – це головний протокол керування мережею TCP/IP. Він був розроблений у 1988 р. Його використовують мережеві програми керування. Він діє ланцюжком SNMP-UDP-IP-фізична мережа.

Найважливішим об'єктом керування є зовнішній порт мережі або маршрутизатор. Кожен об'єкт керування має свій унікальний номер (протокол дає змогу тільки запитувати про стан керованих об'єктів та одержувати інформацію. Зміна параметрів та вирішення проблем відбуваються 'на місці').

SNMP працює на базі протоколу UDP. Він дає змогу станціям керування збирати інформацію про стан мережі. Цей протокол визначає формат даних, а опрацьовують та інтерпретують їх станції керування. SNMP-повідомлення не мають фіксованого формату. Під час роботи протокол SNMP використовує базу даних **MIB** (Management Information Base) (див. Д.22.2).

Типи команд SNMP наведено в табл. Д22.1.1.

Таблиця Д.22.1.1 Типи команд SNMP

Команда SNMP	Тип pdu	Призначення
get_request	0	Одержати значення змінної
get_next_request	1	Одержати значення змінної за наступним ідентифікатором на дереві MIB
set_request	2	Присвоїти змінній конкретне значення
get_response	3	Відповідь на 0,1,2
trap	4	Відповідь мережевого об'єкта на подію

Команди get-типу використовують для одержання інформації, set – для присвоєння значень тим змінним, що допускають це, trap – для повідомлення станції керування про конкретну подію.

Структура SNMP-повідомлень, які вкладаються у UDP-даграми, зображена на рис. Д.22.1.1.

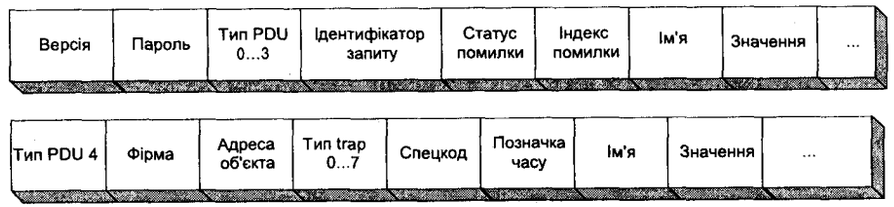


Рис. Д.22.1.1. Структура SNMP-повідомлень.

Поле *Версія* містить номер версії SNMP – 1. *Пароль* – це послідовність символів, що є перепусткою на маршрутизатор. Часто в цьому випадку використовують слово 'public'. *Тип PDU* – це ідентифікатор команди. *Ідентифікатор запиту* встановлює станція керування. Він дає змогу об'єднувати в одне ціле запити та відповіді. Поле *Статус помилки* встановлює об'єкт керування і позначає тип помилки та її значення. Важливою складовою SNMP-пакета може бути ідентифікатор MIB-змінної у цифровому вигляді, наприклад 1.3.6.1.2.1.5

Останнім часом поширилася ідеологія **розподіленого протокольного інтерфейсу** (Distributed Protocol Interface (DPI)). У ньому для транспортування SNMP-повідомлень використовується не тільки протокол UDP, але й TCP. Це дає змогу застосовувати SNMP-керування не тільки в локальних мережах.

Для ілюстрації роботи протоколу SNMP на Unix-системі можна скористатись командою

snmpi -a <адреса>,

де адреса – це адреса одного з гостів або маршрутизаторів мережі, з якого буде зчитуватись інформація. У відповідь на екрані з'явиться підказка

snmpi >

Користувач уводить команди get <позначення об'єкта>, next <позначення об'єкта>, де позначення об'єкта – це символьне ім'я змінної з MIB-бази даних. Якщо змінна проста, до неї додається суфікс 0, наприклад:

get sysDescr.0,

якщо змінна – елемент таблиці, то у суфіксі записують індекс елемента, наприклад:

```
snmpi > next ifTable
snmpi > ifIndex.1=1
snmpi > get ifDescr.1
snmpi > ifDescr.1 = 'Ethernet0'
```

Д.22.2. База даних керування мережею MIB

Уся інформація, яку застосовують для контролю та керування маршрутизаторами і гостами мережі TCP/IP, зберігається в локальних для цих пристроїв базах **MIB** (RFC 1213). Ці дані зчитують та аналізують програми керування мережею з використанням протоколу SNMP.

Відповідно до нормативів MIB інформація наведена у вигляді дерева (рис. Д.22.2.1), де кожен наступний рівень ієрархії є деталізацією попереднього. Інформація про окремі компоненти записана згідно з нотацією **ASN.1** (Abstract Syntax Notation 1). Це формальна мова, яка дає змогу компактно подати компонент дерева.

Окремі компоненти можуть мати такі типи:

- **integer** – ціле значення з можливим визначенням допустимого діапазону значень;
- **octet string** – довільна послідовність байтів; починається з числа – кількості байтів;

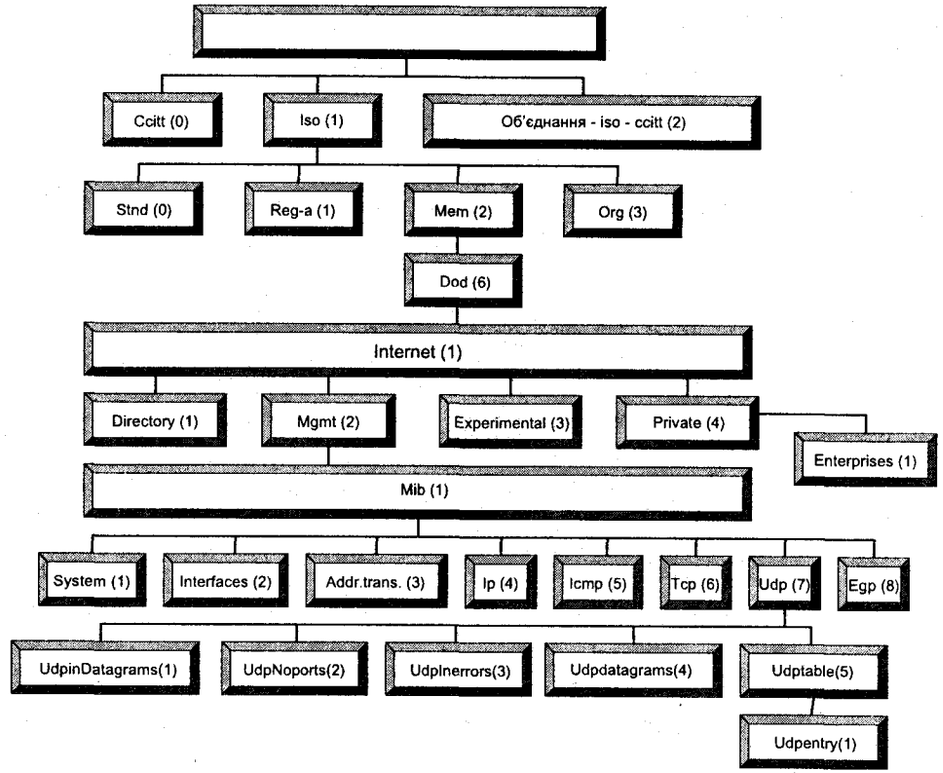


Рис. Д.22.2.1. Структура бази MIB.

- **object identifier** (ім'я об'єкта) – послідовність цілих чисел, розділених крапками; набір цих чисел вказує шлях від вершини дерева до конкретного об'єкта, наприклад, 1.3.6.1.2.1.5;
- **null** – нема значення;
- display string – стрічка з нуль або більше (до 255) символів ASCII; частковий випадок octet string;
- physAdress (послідовність байтів) – фізична адреса об'єкта;
- choice – тип протоколу; сьогодні визначено тільки один тип – Internet;
- IpAdress – 32-розрядна IP-адреса (octet string);
- Time Ticks – додатне ціле число, що визначає час у сотих частках секунди;
- Gauge – масштаб; додатне ціле число в діапазоні $0..2^{32}-1$; може збільшуватися або зменшуватися; переповнення недопустиме;
- Counter – лічильник; додатне ціле число в діапазоні $0..2^{32}-1$; може тільки збільшуватися; переповнення допустиме;
- Sequence – аналог структури; складається з кількох полів, можливо, різного типу;
- Sequence of – вектор, усі елементи якого мають один тип.

Серед можливих типів визначають головні та похідні типи. Головні типи виділені грубим шрифтом.

Елементом бази MIB є також маршрутні таблиці. Кожному маршруту відповідає окрема таблиця (табл. Д.22.2.1).

Таблиця Д.22.2.1. Структура маршрутної таблиці

Місце призначення (ipRoutDest)	IP-адреса кінцевого пункту маршруту
Індекс інтерфейсу (ipRouteIfIndex)	Фізичний порт, на який відбудеться передавання
Метрика 1 (ipRouteMetric1)	Оцінка маршруту 1
....	
Метрика 5 (ipRouteMetric5)	Оцінка маршруту 5
Наступний крок (ipRouteNextHop)	IP-адреса наступного маршрутизатора
Тип маршруту (ipRouteType)	3 - мета маршруту досягається безпосередньо, 4 - з проміжними кроками, 2 - маршрут не можна реалізувати, 1 - інше
Протокол маршрутизації (ipRouteProto)	Код протоколу: 8 - RIP, 13 - OSPF, 14 - BGP, 4 - ICMP, 1 - інші
Вік маршруту (ipRouteAge)	Час з моменту останньої корекції маршруту
Маска маршруту (ipRouteMask)	Значення для логічної побітової операції 'І' над адресою в даграмі. Результат порівнюється з адресою в полі 'Місце призначення'
Маршрутна інформація (ipRouteInfo)	Код, що залежить від протоколу маршрутизації і містить посилання на іншу інформацію в MIB

Д.22.3. RMON та керування у корпоративних мережах

Глобальні корпоративні мережі та дистанційний моніторинг. У глобальних корпоративних мереж проблеми віддаленого керування та моніторингу посідають важливе місце. Чому?

- У глобальних мережах велика вартість ліній зв'язку. Засоби зменшення завантаженості та оптимізації швидко окупляються.
- Велика різноманітність платформ та систем спричинює додаткові складності у процесі діагностування та керування.
- Великі відстані між центральним офісом та філіями. Віддалене керування дає змогу налагоджувати обладнання без виїзду на місце. Економія на утриманні кваліфікованого персоналу та відрядженнях.
- Розподіл функцій та центрів керування мережею дає змогу спростити та здешевити керування.

Вимоги до систем керування. Засоби керування повинні стежити за трафіком та іншими параметрами без 'засмічення' мережі великою кількістю службової інформації, бути достатньо інтелектуальними та самостійно визначати стан мережевих пристроїв і, якщо не самостійно ремонтувати їх, то хоча б самостійно діагностувати несправності та попереджувати працівників

ремонтних служб. Бажано, щоб засоби керування попереджали про можливі проблеми ще до їх виникнення. Однак такі 'ідеальні' вимоги до систем керування далекі до реалізації, та певним етапом на цьому шляху стала розробка стандарту RMON.

Загальна характеристика RMON. RMON є подальшим удосконаленням SNMP. Агенти SNMP не опрацьовують та не узагальнюють інформації. Агенти RMON деякою мірою можуть виконувати ці функції. Стандарт RMON (RFC-1271 – Remote Network Monitoring Management Base, листопад 1991 р.) містив опис баз даних RMON для мереж Ethernet. Пізніше з'явився стандарт для мереж Token Ring (RFC-1513). У лютому 1995 р була опублікована нова версія базового стандарту з номером RFC-1271.

Інформацію про мережу збирають програмно-апаратні агенти. Вони передають інформацію на застосування керування мережею. Агенти SNMP за запитом цієї програми надсилають інформацію про функціонування того пристрою, де вони встановлені. Зрозуміло, що така схема інформаційного обміну може дуже перевантажити мережу. Особливо це стосується глобальних мереж з дорогою перепускною здатністю.

Агенти RMON самостійно опрацьовують дані і надсилають вже частково опрацьовану інформацію. Вони можуть фільтрувати потік, збирати дані про відхилення від базового рівня функціонування, повідомляти віддаленого адміністратора про визначені події.

Структура інформаційної бази RMON. Відповідно до RFC-1271 інформаційна база RMON складається з десяти груп даних.

1. *Група статистики (statistics)*. Накопичується інформація про трафік сегмента, ступінь використання перепускної здатності мережі, статистика помилок тощо.
2. *Група передісторії (history)*. Збирання інформації, визначеної в групі статистики, на заданому часовому інтервалі. Можливість порівняння за часом та з базовими значеннями.
3. *Група аварійних сигналів (alarms)*. Дає змогу користувачу визначити низку граничних значень, у випадку перевищення яких генерується аварійний сигнал. Можливе гнучке комбінування параметрів, одержання параметрів з інших груп. Аварійний сигнал передається у групу подій.
4. *Група гостів (hosts)*. Реєструють усі гост-машини та інші пристрої в цьому сегменті.
5. Окремо виділяється *таблиця N головних гостів (HostTopN)* – гостів, які мають максимальне значення заданого статистичного параметра на заданому інтервалі. Таблицю складає сам агент, а програма керування одержує тільки результат.
6. *Матриця трафіку (traffic matrix)*. Рядки цієї матриці відповідають MAC-адресам станцій-джерел повідомлень, а стовпці – одержувачам повідомлень у сегменті. У матрицю записується інтенсивність трафіку між станціями та кількість помилок у ньому. Матрицю формує сам агент.
7. *Фільтри (filters)* використовують для фільтрування пакетів. Ознаки фільтрування можуть бути комбінованими і досить складними. Наприклад, помилковими можуть вважатися пакети, довжина яких перевищує конкретне значення. У цьому випадку можна задати канал, куди будуть передаватися вибрані пакети (наприклад, у буфер). Поява пакета з визначеною ознакою може вважатися подією, на яку система реагує визначеним чином.

8. *Група перехоплення пакетів (packet capture)*. Сюди належать буфери, що приймають пакети з визначених фільтрів. У цьому випадку пакет може бути перехоплений не цілим, але визначеною частиною (наприклад, заголовок). Зміст буферів аналізують пізніше програмні засоби з метою виявлення тенденцій.

9. *Група подій (events)* визначає, як реагувати на різні події. Наприклад, як реагувати на аварійний сигнал – повідомити систему керування або просто запротоколювати. Спрямування пакета в буфер перехоплення також вважається подією.

10. *Група параметрів Token Ring*.

Подальший розвиток RMON. Агенти RMON збирають інформацію в межах своїх сегментів мережі. Вони не виконують функції аналізу та узагальнення для складних багатосегментних мереж. Тому є потреба в інтелектуальних агентах, які б виконували ці функції. Такі агенти описує стандарт RMON 2, який спочатку мав з'явитися в листопаді 1995 року, потім – наприкінці 1996 року. Однак і досі цей стандарт не розроблено. У RMON 2 буде описаний механізм збирання даних про роботу мережі на мережевому рівні та рівні застосувань.

Як працює та реалізовано RMON. Інформації RMON збирають програмно-апаратні зонди. Такий зонд повинен мати достатні (значні) обчислювальні та запам'ятовувальні ресурси. Розрізняють зонди трьох типів: *вбудовані*, *зонди на базі комп'ютера* та *автономні*. Вважають, що продукт підтримує RMON, якщо в ньому реалізовано хоча б одну групу RMON. Чим більше груп RMON реалізовано у продукті, тим він дорожчий.

Вбудовані зонди – це модулі, які вбудовують у концентратори, комутатори, маршрутизатори. Вони недорогі і працюють з деякою підмножиною груп RMON, однак продуктивність їхня невелика.

Зонди на базі комп'ютера – це комп'ютери з програмним агентом RMON. Такі зонди працюють швидше від вбудованих, підтримують більше груп. Вони дорожчі від вбудованих, проте дешевші від автономних.

Автономний зонд – це спеціалізована машина. Такі зонди невеликі та мобільні. Вони мають найвищу продуктивність і найдорожчі. Часто такі зонди віддають в оренду.

Web-технології керування мережами. Деякі виробники програмного та апаратного забезпечення (Cisco, Compaq, Intel) пропагують перехід до web-засобів керування мережами, аргументуючи це зменшенням витрат та спрощенням. Групу **WBEM** (Web-based enterprise management) підтримує ще 70 фірм.

Концепція WBEM пропонує три рівні стандартизації. Перший – *HMMS (Hyper Media Management Schema)* – визначає модель даних для відображення об'єктів. Другий – *HMMP (Hyper Media Management Protocol)* – протокол, що базується на HTTP для підтримки зв'язків між службами, застосуваннями та агентами. Третій – *HMOM (Hyper Media Object Manager)* – об'єктний C++ диспетчер, що організовує обмін даними між застосуваннями. В основі HMOM є OLE Microsoft.

Д.22.4. Мережеві аналізатори фірми Network General

Одним з можливих еволюційних вирішень реалізації системи керування мережею є поступова інтеграція спеціальних засобів аналізу, діагностики в єдину систему на платформі мережевого керування (наприклад, SunNet Manager, HP Open View, IBM NetView, Novell NMS). Більшість виробників мережевого обладнання випускає системи, якими можна керувати з використанням SNMP або RMON.

Головні функції керування поділяють на функції керування елементами та функції керування комунікаціями.

Керування елементами передбачає таке:

- керування конфігурацією (реєстрація пристроїв та присвоєння їм адрес, визначення параметрів мережевої ОС та протоколів, графічне відображення мережі);
- керування безпекою (контроль доступу та керування повноваженнями користувачів, контроль міжмережевої взаємодії, керування цілісністю даних);
- керування ресурсами (реєстрація ліцензій, облік використання мережевих ресурсів, керування пріоритетами користувачів).

Керування комунікаціями – це:

- опрацювання збоїв (шукання, локалізація помилок, профілактика, контроль кабельної системи);
- керування продуктивністю (збирання статистики про функціонування мережі, аналіз трафіку, виявлення вузьких місць, планування розвитку мережі, її сегментації).

Загальна характеристика продуктів Network General. Найвідомішою фірмою, що спеціалізується на випуску продуктів аналізу мереж, є Network General. Ця фірма охоплює сьогодні понад 50% світового ринку аналізаторів. Їй належать найпередовіші щодо використання експертних систем та масштабованості вирішення. Водночас, що стосується деяких параметрів (наприклад, швидкодії, можливості аналізувати весь трафік, а не його вибірку, особливо у швидкісних мережах), то її продукти уступають продуктам інших фірм.

Сьогодні фірма пропонує дві категорії продуктів:

- **Distributed Sniffer System (DSS)** – складну розподілену систему моніторингу стану мережі з функціями експертного аналізу та віддаленого моніторингу;
- портативні аналізатори для мереж Ethernet, Token Ring, FDDI.

Система *Distributed Sniffer System* (рис. Д.22.4.1) складається з центральної консолі та пристроїв, що перехоплюють й аналізують трафік в окремих сегментах. Вона працює з агентами RMON або SNMP. Розрізняють два типи агентів: агенти моніторингу та агенти аналізу.

Підсистема моніторингу має агенти-монітори двох типів – *Cornerstone Probe* та *Cornerstone Agent*. Функції консолі виконує програма *Foundation Manager*, що інтегрується в платформи керування, такі як HP Open View, однак може працювати і самостійно.

Крім виконання функцій моніторингу, Foundation Manager надає засоби аналізу та нала-

годження продуктивності, відображення графічної схеми обміну на основі трафіку в реальному масштабі часу, дає рекомендації щодо вирішення проблем.

Агент-монітор Cornerstone Agent встановлюють на робочу станцію з MS Windows або OS/2. Він виконує функції SNMP та RMON-агента свого сегмента. Другий агент-монітор Cornerstone Probe – це Cornerstone Agent, встановлений на безмоніторний ПК (призначений). Кожен з цих агентів використовує до 4080 фільтрів.

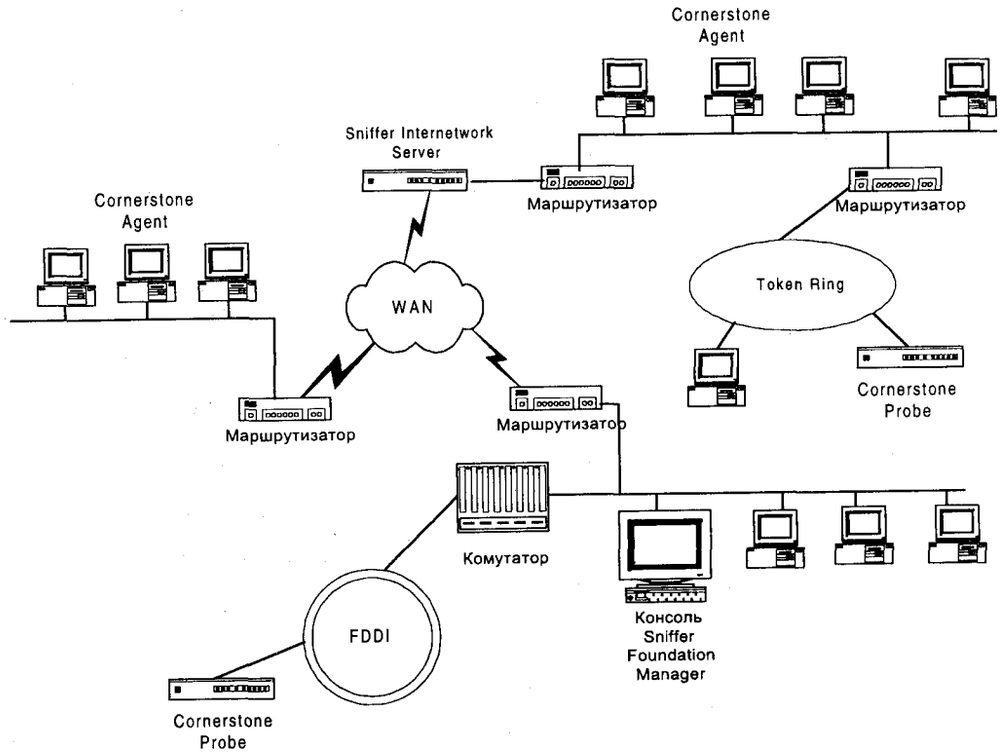


Рис. Д.22.4.1. Структура системи керування та аналізу DSS.

Підсистема аналізу складається з ПЗ центральної консолі *Sniffer Master Console (SMC)* та двох типів агентів-аналізаторів – *Sniffer Server (SS)* і *Sniffer Internetwork Server (SIS)*. SMC може працювати самостійно або бути інтегрована в платформу керування. SS – головний елемент підсистеми аналізу. Він аналізує та інтерпретує протоколи, передає інформацію на SMC. SS реалізовано на спеціалізованому апаратному блоці. Головні його функції: автоматична побудова конфігурації сегмента, підтримка конфігурації в актуальному стані, ідентифікація аномальних

подій на всіх рівнях протоколу та надання рекомендацій щодо їх усунення, інтерпретація понад 200 протоколів, автоматична генерація звітів. SS має експертну систему, в основі якої є база знань, що постійно поповнюється. Експертна система генерує такі три категорії діагностичної інформації:

- симптом – опис події в мережі, якій адміністратор повинен приділити увагу;
- діагноз – опис симптомів, що повторюються і які обов'язково повинен вивчити адміністратор;
- пояснення – контекстно-залежний експертний висновок системи для кожного симптому чи діагнозу; містить опис кількох можливих причин.

SIS працює аналогічно до SS, однак призначений для аналізу міжсегментних та міжмережевих зв'язків. Головне призначення SIS – аналіз та оптимізація використання дорогих зовнішніх ліній зв'язку.

Портативні системи Expert Sniffer Analyser надають адміністратору ті ж можливості, що й DSS, проте для одного сегмента.

Як свідчить досвід зарубіжних компаній, системи аналізу окупляють себе протягом перших місяців експлуатації. У цьому випадку час простою мережі зменшується в середньому на 28%, а в адміністраторів вивільняється понад 50% часу, який витрачався на усунення несправностей.

Д.22.5. Система IOS – вирішення фірми Cisco з забезпечення якості передавання

Зростання комп'ютерних мереж, розвиток мережевих технологій, популярність та потужність Internet залучили до мережі багато користувачів та багато застосувань з різними вимогами до параметрів передавання. Постала проблема оптимального керування різнотипними інформаційними потоками. Її можна вирішити, впровадивши відповідні процедури в усіх проміжних ланках та пристроях передавання та координуючи їхню роботу. Не дивно, що фірма Cisco, як провідний виробник активного обладнання для магістральних телекомунікаційних та корпоративних мереж, мала унікальні можливості щодо розробки та впровадження засобів *керування якістю передавання*.

Комплекс вирішень Cisco – це програмне забезпечення IOS, що складається з багатьох компонент, які працюють на активних пристроях цієї фірми, та декількох інших продуктів для координації та адміністрування.

Керування якістю передавання дає змогу:

- *керувати ресурсами* (наприклад, можна надати перевагу застосуванням роботи з базами даних, а не передаванню файлів);
- *ефективніше використовувати ресурси* (застосовуючи засоби аналізу та адміністрування, можна бачити як справді мережа обслуговує найважливіші потоки);
- *диференціювати послуги* (маючи змогу надати гарантовані параметри QoS, мережевий провайдер може визначити різні класи обслуговування);

• *забезпечити співіснування різних за важливістю застосувань* (засоби QoS можуть гарантувати, що менш важливі застосування не впливатимуть на параметри мережевих сполучень критично важливих застосувань);

• *закласти основу для повністю інтегрованих мереж майбутнього.*

У роботі засоби IOS використовують можливості пріоритетного керування передаванням, закладені в наявні протоколи, зокрема:

• поле *Service type* IP v4-пакета та три біти пріоритету в ньому, які дають змогу задавати значення пріоритету 0–7 (див. 13.1);

• поля *FECN*, *BECN*, *DE* мережі Frame Relay, які дають змогу керувати перевантаженнями та відкидати пакети (див. 22.7);

• визначення класу сервісу мережі ATM (див. 29.4);

• протоколи ізохронного передавання та резервування ресурсів RTP та RSVP (див. Д.13.10);

• розширення протоколу PPP (див. Д.13.4) – Multilink PPP, який дає змогу фрагментувати довгі кадри та використовувати декілька ліній одночасно, що збільшує вислідну швидкість передавання.

Складові частини підсистеми забезпечення QoS вирішують такі завдання:

• керування в умовах перевантаження (диспетчеризація та опрацювання черг);

• прогнозування та уникнення перевантажень;

• керування потоком;

• підвищення ефективності ланки зв'язку;

• координація та сигналізування діяльності пристроїв на шляху потоку;

• аналіз якості обслуговування та адміністрування компонент системи.

Розглянемо їх окремо.

Засоби керування в умовах перевантаження, головним чином, охоплюють механізми опрацювання черг пакетів. Засоби IOS підтримують такі процедури опрацювання черг:

• *перший на вході – перший на виході (**FIFO**)*;

• *черги з пріоритетами (Priority Queuing (**PQ**))*;

• *пропорційний розподіл смуги перепускання (Custom Queuing (**CQ**))*;

• *розподіл з ваговими коефіцієнтами (Weighted Fair Queuing (**WFQ**))*.

Кожна з дисциплін опрацювання черг призначена для вирішення конкретної проблеми керування потоком і впливає на його параметри.

FIFO – це базова, первинна дисципліна опрацювання пакетів у черзі. Якщо виникло перевантаження, то пакети накопичуються у буфері, а потім передаються з нього в порядку їх надходження. Така схема не підтримує пріоритетності пакетів, може призвести до недопустимих затримок важливих потоків, захоплення перепускної здатності системи одним потоком. Вирішення IOS передбачають інтелектуальніші підходи до керування чергами.

У **чергах з пріоритетами (PQ)** конкретним інформаційним потокам надають пріоритет перед іншими. Пріоритет може визначатися за вживаними протоколами, портами надходження пакетів, адресами відправника й одержувача та ін. Пакети надходять в одну з чотирьох черг

(високого, середнього, нормального та низького пріоритетів). Алгоритм опрацювання черг найперше обслуговує пакети з черг вищих пріоритетів, і тільки у разі їх звільнення переходить до черг нижчого пріоритету. (рис. Д.22.5.1).

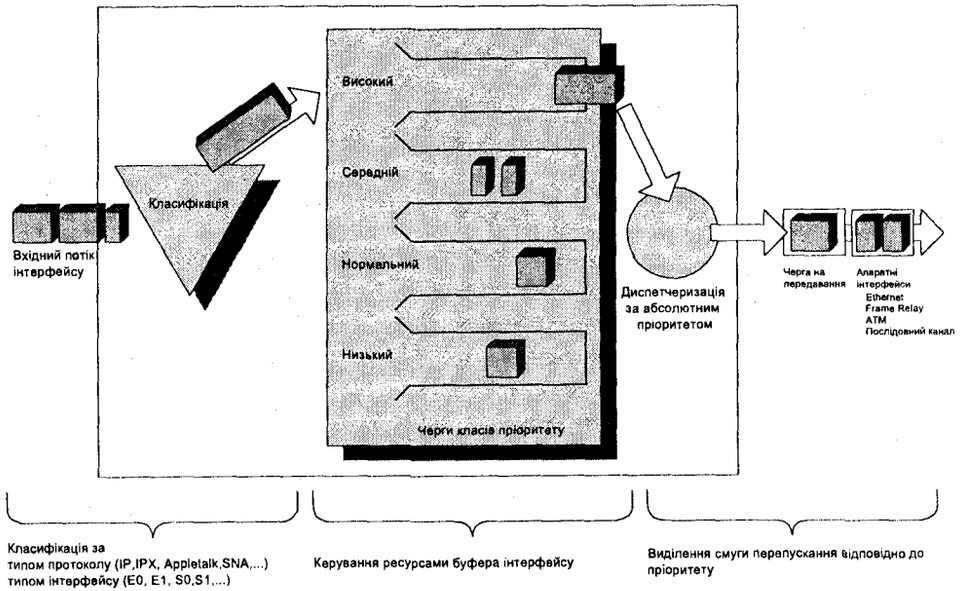


Рис. Д.22.5.1. Опрацювання пакетів у чергах з пріоритетами.

Такий механізм є простим, однак його використання призводить до непередбачуваної затримки пакетів менших пріоритетів. На практиці доводиться обмежувати потік пріоритетних пакетів. Схему черг з пріоритетами використовують там, де потрібно гарантувати першочергове обслуговування важливого потоку. PQ не адаптується до зміни стану мережі, а налаштовується статично.

У механізмі з пропорційним розподілом смуги перепускання кожному потоку, якщо виникло перевантаження, надається деяка мінімальна гарантована смуга перепускання. Загальна смуга перепускання пропорційно розподілена між потоками (рис. Д.22.5.2).

Відповідно до розподілу смуги перепускання визначено 17 черг. У чергу 0 потрапляють пакети системного керування та сигналізування, а в черги 1–16 – пакети користувачів. Диспетчер передавання почергово опрацьовує всі черги пропорційно до їхньої частки у загальній смузі перепускання. Таким чином гарантовано мінімальний рівень опрацювання потоку якщо виникло перевантаження. Аналогічно до PQ CQ не адаптується до зміни стану мережі.

Розподіл з ваговими коефіцієнтами (WFQ) – це інтелектуальна процедура, яка дає змогу передавати потоки різної інтенсивності в різних умовах навантаження. У цьому випадку

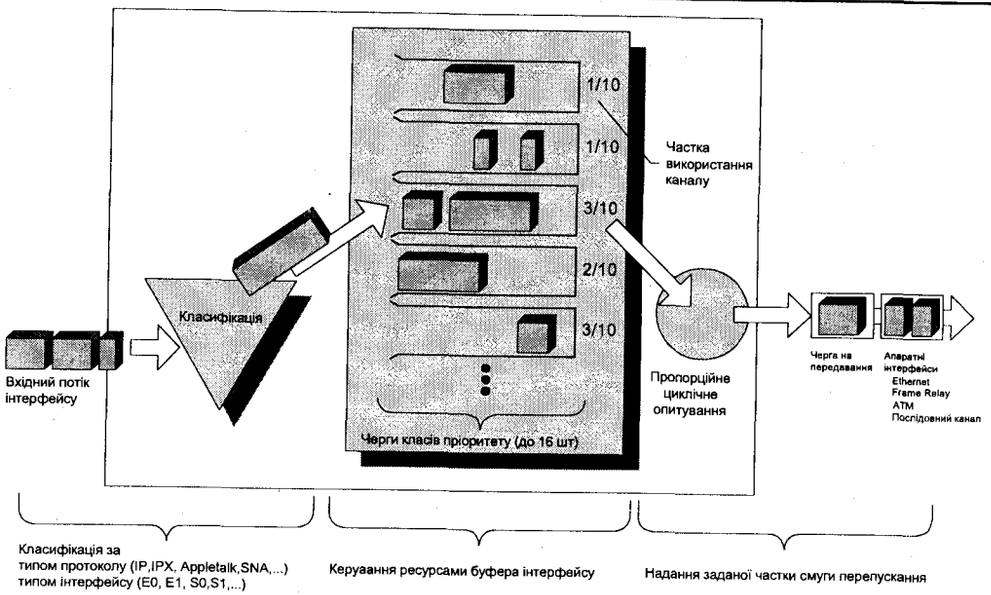


Рис. 22.5.2. Опрацювання пакетів для пропорційного розподілу смуги перепускання.

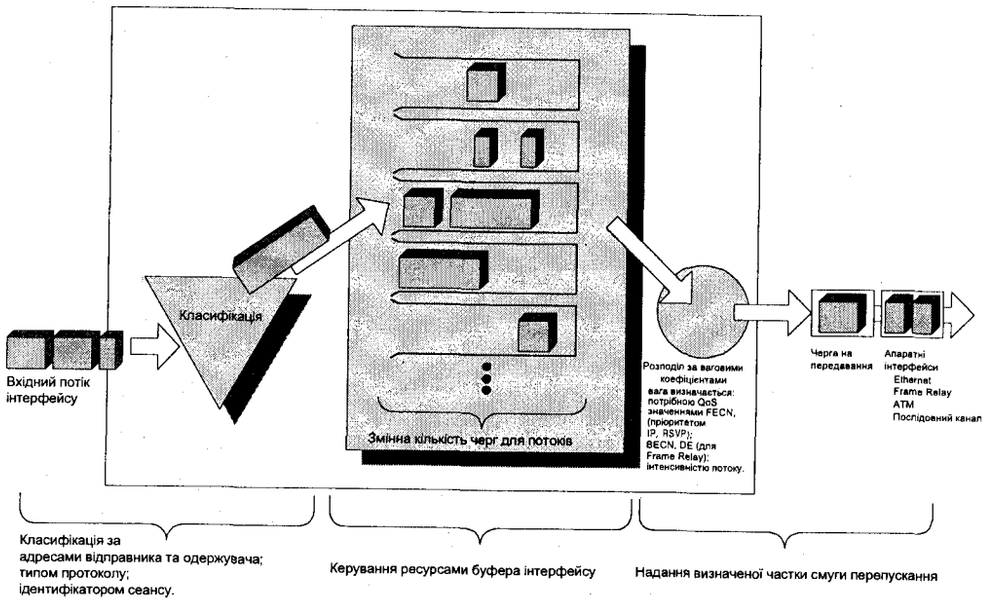


Рис. Д.22.5.3. Опрацювання пакетів процедурою зваженого розподілу.

пріоритет надається інтерактивним потокам з невеликими обсягами передавання. Решту смуги перепускання розділяють між собою пропорційно потоки значних обсягів (рис. Д.22.5.3).

WFQ потребує мінімальних витрат на налаштування та динамічно адаптується до стану мережі. Якщо немає високопріоритетного трафіку, WFQ дає змогу використовувати всю смугу перепускання низькопріоритетним потокам.

WFQ використовує поле пріоритетів IP-пакета. Чим більше значення пріоритету, тим меншу частку перепускної здатності одержить пакет. RSVP використовує WFQ для призначення смуги перепускання визначеним потокам та розміру буферів. У мережах Frame Relay пристрої з WFQ враховують поля кадрів *FECN*, *BECN*, *DE*. Якщо вони сигналізують про перевантаження, то пакети відповідного потоку передаються рідше.

Прогнозування та уникнення перевантажень. На відміну від засобів роботи в умовах перевантажень, засоби прогнозування та уникнення перевантажень стежать за мережевими потоками і намагаються запобігти виникненню перевантажень. Головний засіб уникнення перевантажень в IOS – це *Weighted Random Early Detection (**WRED**)*. В основі цього методу є механізм **RED**, який полягає в тому, що в критичних точках мережі постійно вимірюється інтенсивність потоку і, якщо вона наближається до порогу перевантаження, деякі пакети відкидають, зменшуючи таким чином навантаження. Вибір пакетів виконується випадково. Джерело пакетів виявляє їхню втрату й інтерпретує її як потребу зменшити темп передавання. WRED – це модифікація RED, розроблена Cisco. У ній враховано поле пріоритету IP-пакета так, що у випадку виникнення перевантаження відкидаються пакети з низьким пріоритетом (рис. Д.22.5.4).

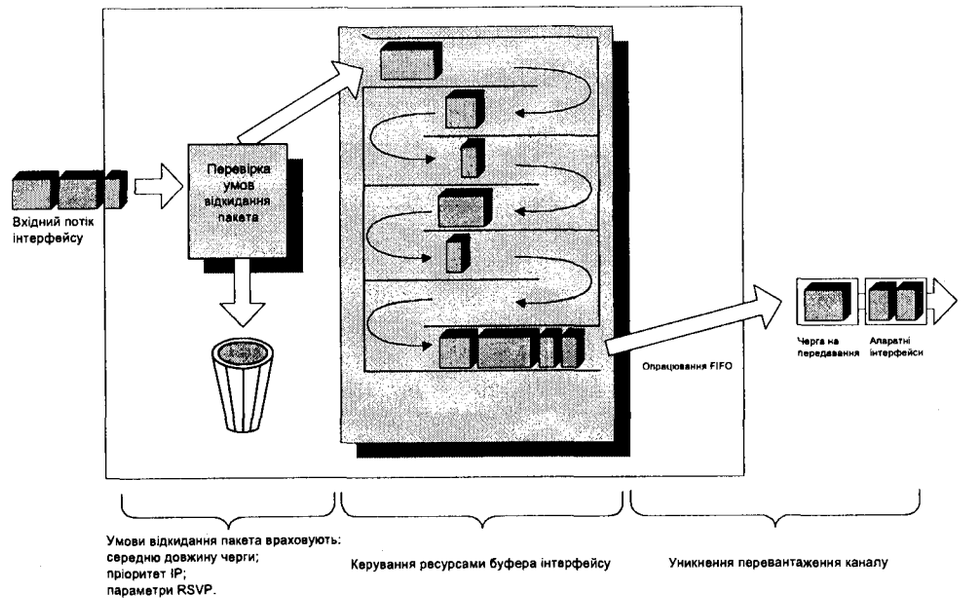


Рис. Д.22.5.4. Механізм WRED.

Засоби керування потоком IOS визначають два підходи:

- базовий (Generic Traffic Shaping (**GTS**));
- керування потоком мережі Frame Relay (Frame Relay Traffic Shaping (**FRTS**)).

Базовий механізм керування потоком обмежує інтенсивність вихідного потоку конкретного інтерфейсу певним значенням. У цьому випадку згладжуються різкі коливання інтенсивності потоку, а надлишок пакетів затримують у буфері. Таким чином налаштовують взаємодію інтерфейсів різної швидкості (рис. Д.22.5.5).

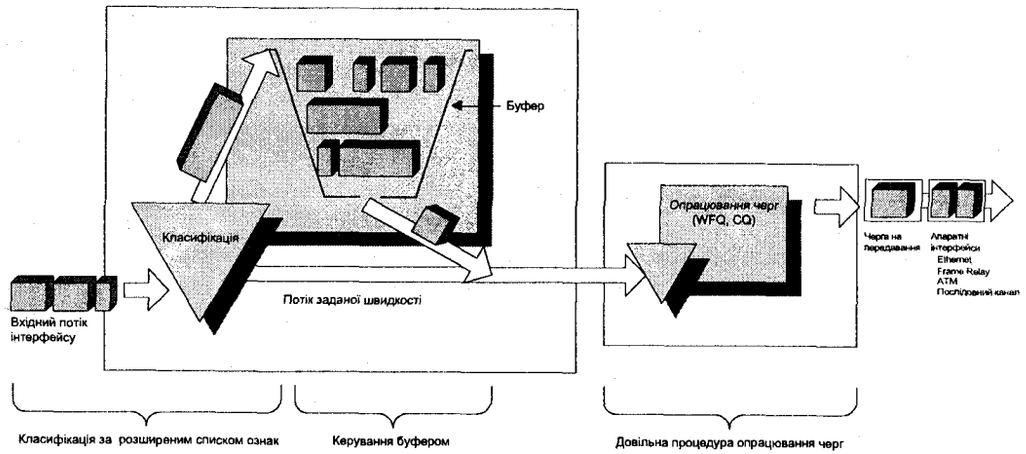


Рис. Д.22.5.5. Базовий механізм керування потоком.

GTS працює з різними технологіями канального рівня, такими як Ethernet, ATM, Frame Relay та ін.

Механізм FRTS враховує додаткові засоби керування потоком мережі Frame Relay: гарантовану швидкість передавання CIR, повідомлення про перевантаження (FECN, BECN), біт можливості знищення DE. Використання FRTS дає змогу значно підвищити ефективність сполучення Frame Relay, зменшити тривалість відповіді, зробити керування точнішим. Наприклад, можна обмежити швидкість передавання пакетів значенням CIR або довільним іншим значенням для кожного віртуального каналу окремо. Використовуючи значення поля BECN, FRTS *може гальмувати інтенсивність потоку для кожного віртуального каналу.*.

Засоби підвищення ефективності ланки зв'язку. В IOS використовують два механізми підвищення ефективності ланки зв'язку:

- стиснення заголовка протоколу RTP (Real Time Protocol Header Compression (RTP-HC));
- фрагментування та чергування кадрів каналу (Link Fragmentation and Interleaving (**LFI**)).

Стиснення заголовка пакетів протоколу RTP дає найбільший ефект у деяких нових мультимедійних застосуваннях, таких як IP-телефонія. RTP-пакет має заголовок завдовжки 40 байт та інформаційну частину – 20–150 байт. Враховуючи додаткову довжину UDP- та IP-

заголовків передавати такий пакет стає невигідно. Стиснення дає змогу зменшити сукупну довжину заголовків RTP/UDP/IP до 2–5 байт, що дає відчутний ефект для застосувань з трафіком невеликих пакетів низькошвидкісними лініями зв'язку (рис. Д.22.5.6).

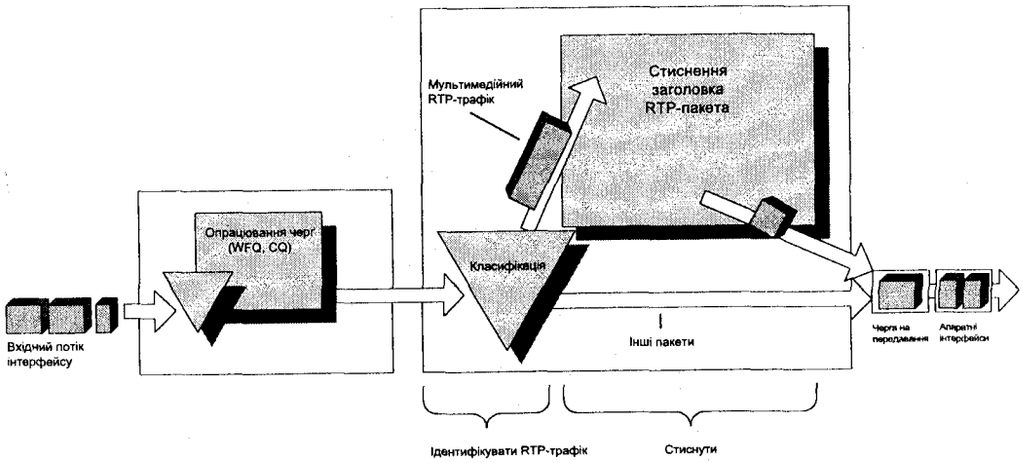


Рис. Д.22.5.6. Стиснення RTP-заголовка.

Фрагментування та чергування кадрів канального рівня також вигідне для низькошвидкісних сполучень. На час відповіді деяких інтерактивних застосувань, що працюють з короткими пакетами, можуть суттєво вплинути великі пакети інших застосувань, що передають тим же каналом. Тому система аналізує розміри кадрів, що надходять. Якщо кадр є великим, а в черзі чекають невеликі кадри інтерактивних застосувань, то великі кадри фрагментують і передають частинами, а в проміжках між ними – невеликі кадри інтерактивних застосувань (рис. Д.22.5.7). LFI підтримує протокол Multilink PPP.

Засоби координації та сигналізування дають змогу повідомляти пристрої мережі про потрібну якість обслуговування потоку. Разом з процедурами, які працюють на окремих пристроях, вони мають на меті забезпечити наскрізне дотримання параметрів QoS. Для цього необхідно, щоб кожен компонент мережі на шляху пакета(гост, комутатор, маршрутизатор, брандмауер) забезпечував єдині параметри якості обслуговування. Механізмів для забезпечення координації є багато, однак найчастіше вони мають обмежену сферу дії. Ще складніше забезпечити координацію в об'єднанні різнотипних мереж.

У вирішеннях Cisco ґрунтується на універсальності протоколу IP і використовує пріоритет у його пакетах для забезпечення вибіркового обслуговування і засоби протоколу RSVP для надання гарантованих послуг. Крім того, Cisco використовує можливості координації якості обслуговування мереж ATM та Frame Relay.

Біти пріоритету в полі *Service Type* IP-пакета дають змогу вибрати один з шести класів сервісу (ще два класи використовує система). Користувач може визначати пріоритет залежно від типу застосування, протоколу, потрібної швидкості передавання та ін.

Протокол RSVP – єдиний стандартизований сьогодні засіб для забезпечення гарантованої якості обслуговування. Засобами, які реалізують дотримання визначених параметрів якості, є WFQ та WRED.

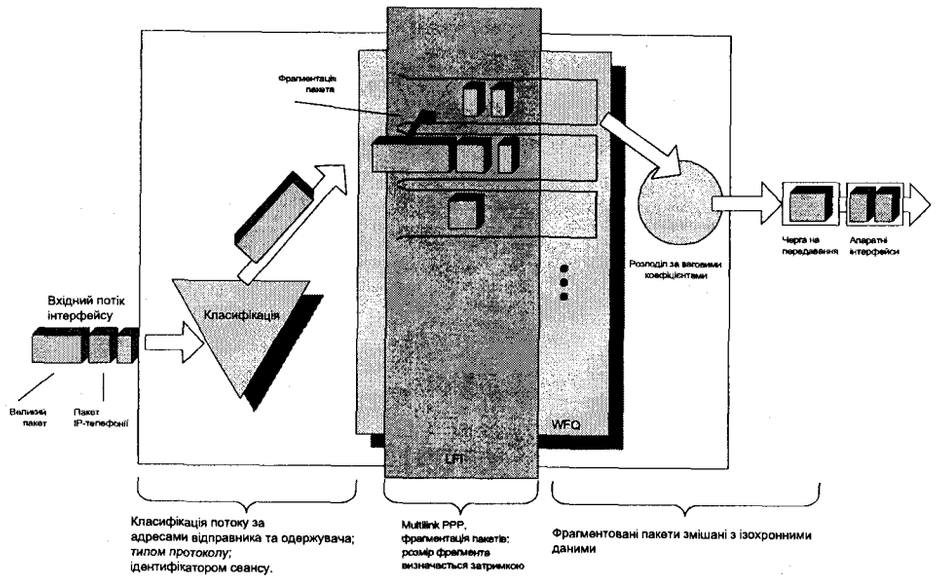


Рис. Д.22.5.7. Фрагметування та перемішування кадрів.

Аналіз якості обслуговування та адміністрування вирішує такі завдання:

- керування пріоритетністю;
- автоматизації аналізу, діагностування та налаштування параметрів;
- моніторингу, мережеметрії та аналізу вартості.

Засоби керування пріоритетністю реалізує IOS згідно з архітектурною концепцією *CiscoAssure*. Вони дають змогу проводити приорітетну політику з єдиної консолі адміністратора. В основі такої політики є процедури класифікування пакетів, на підставі яких пакету можна присвоїти певний клас обслуговування. Керування пріоритетністю потребує також інтеграції з засобами канального рівня та інших типів мереж і протоколів.

Наприклад, для взаємодії з мережами IBM архітектури SNA використовують механізм пріоритезації пакетів і технологію передавання SNA-трафіку через IP-мережі SNA ToS та Data Link Switching+ (DLSw+), які дають змогу відобразити параметри якості сервісу протоколів SNA (SNA Class-of-Service – CoS) у параметри пріоритету протоколу IP. У цьому випадку весь

потік SNA-пакетів поділяють на чотири потоки і кожному з них призначають свій рівень пріоритету.

Керування пріоритетністю реалізовано також у пріоритетній маршрутизації (Policy based routing (**PBR**)). Вона дає змогу визначати для різних за пріоритетами потоків різні маршрути в мережі, що робить маршрутизацію гнучкішою.

Подібним до PBR є підхід керування пріоритетами з використанням заданої середньої інтенсивності надходження пакетів (Commited Access Rate (**CAR**)). Для конкретного інтерфейсу аналізується потік або його підмножина, і, якщо інтенсивність надходження пакетів перевищує значення CAR, зменшується пріоритет потоку.

Засоби автоматизації аналізу, діагностування та налаштування параметрів є в наборі продуктів Cisco Netsys Service-Level Management Suite 4.0:

- Cisco Netsys Connectivity Service Manager;
- Cisco Netsys Performance Service Manager;
- Cisco Netsys LAN Service Manager.

Cisco Netsys Connectivity Service Manager – це перший з цілої серії продуктів, які використовують імітаційне моделювання. Він призначений для допомоги мережевим аналітикам у вирішенні проблем мережевих сполучень, аналізу потоків, маршрутизації.

Cisco Netsys Performance Service Manager використовує моделювання для оцінки параметрів функціонування мережі, планування її роботи, допомагає вирішити проблеми продуктивності мережі. Використовуючи цей засіб адміністратор, може на підставі конфігураційних та тестових даних визначити базовий рівень мережі і потім досліджувати вплив на нього змін у топології, розподілі потоків, маршрутній політиці, інших параметрів. Тут також можна вирішувати проблеми функціонування мережі, налаштовувати параметри на найвищу продуктивність мережі, планувати етапи модифікації.

Засоби моніторингу, мережеметрії та аналізу вартості представлені продуктами NetFlow та Cisco Enterprise Accounting (CEA).

NetFlow ідентифікує, оцінює та збирає інформацію про наявні у мережі потоки. Зібрані дані передаються іншим програмам для опрацювання.

Cisco Enterprise Accounting призначений для оцінювання та керування вартістю перепускної здатності мережі. Він дає змогу адміністратору оцінити витрати на функціонування мережевих компонент, зрозуміти структуру та взаємозв'язок цих витрат, і в результаті зменшити вартість експлуатації мережі.

Приклади використання IOS

Одним з найголовніших завдань підсистеми забезпечення QoS в IOS є *пріоритетне передавання* критично *важливих* для організації *інформаційних потоків*.

Система збуту у філіях фармацевтичної компанії (рис. Д.22.5.8) потребує оперативного доступу до бази даних Oracle у головному офісі фірми. Сполучення виконується з використанням мережі Frame Relay. Цю ж мережу використовують інші застосування фірми. В зв'язку зі

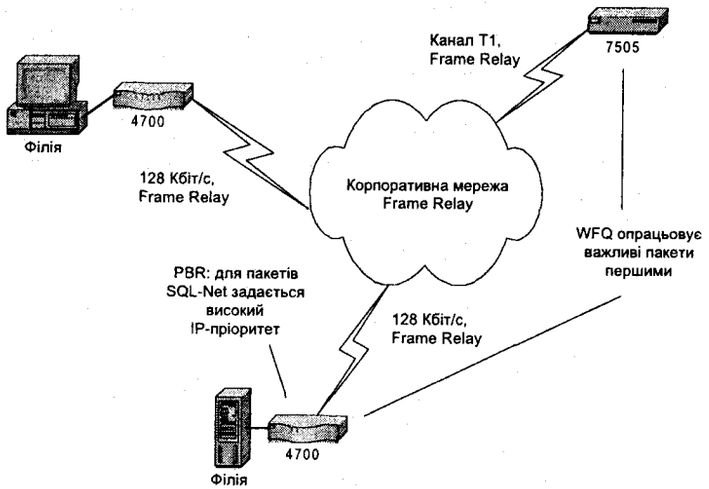


Рис. Д.22.5.8. Мережа фармацевтичної компанії.

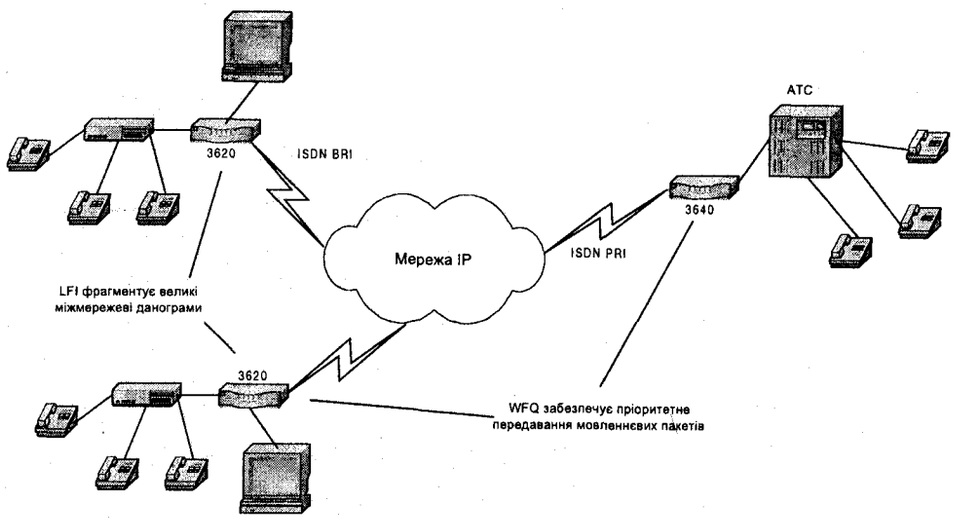


Рис. Д.22.5.9. Передавання мовленнєвих повідомлень.

швидким зростанням корпоративної intranet-мережі, збільшенням кількості її користувачів, створенням додаткових інформаційних потоків робота застосувань збуту сповільнилася внаслідок перевантаження мережевих каналів. Керівництво фірми вважає, що застосуванням збуту повинен бути наданий пріоритет. Вирішення цієї проблеми зводиться до використання у маршрутизаторах філій фірми механізмів пріоритетної маршрутизації (PBR), які для пакетів протоколу Oracle SQL-Net задають високий IP-пріоритет. Проміжні маршрутизатори підтримують механізм опрацювання черг WFQ, що забезпечує пріоритетне передавання пакетів з високим IP-пріоритетом. Маршрутизатор офісу фірми також розпізнає ці пакети.

Однією з найперспективніших мережевих технологій сьогодення є *передавання телефонних розмов через мережу IP* (IP-телефонія). Вона може суттєво зменшити вартість телефонних розмов. Cisco розробила низку продуктів для реалізації IP-телефонії. Водночас для передавання таких повідомлень мережею потрібно впровадити засоби їх пріоритетного передавання.

Розглянемо приклад компанії, яка вирішила зекономити на оплаті телефонів, спрямувавши частину свого мовленєвого трафіку в IP-мережу (рис. Д.22.5.9). На робочих місцях сигнал мовлення оцифровується і передається на пристрій H.323 Gatekeeper, який збирає мовленєвий трафік з декількох телефонів, опрацьовує його, передає на маршрутизатор і задає для нього високий IP-пріоритет. Маршрутизатори мережі підтримують цей пріоритет засобами WFQ. Оскільки IP-мережа була спроектована для передавання даних, то довжина пакетів у ній може досягати 1500 байт. Передавання таких великих пакетів (особливо низькошвидкісними каналами) може призвести до затримок пакетів IP-телефонії і погіршення якості сигналу мовлення. Тому на маршрутизаторах використовують LFI для дефрагментування та чергування пакетів.

Розділ 23

СЛУЖБИ КАТАЛОГІВ КОМП'ЮТЕРНИХ МЕРЕЖ

Поняття 'служби каталогів' та її головні властивості. Історія розвитку. Ієрархічна та доменна архітектури. Служба каталогів NDS.

23.1. Поняття 'служби каталогів' та її головні властивості

Потреба підтримки спеціальних служб каталогів комп'ютерних мереж зумовлена значним зростанням мереж, наявністю в них багатьох серверів різного профілю, великої кількості користувачів. Що ж таке служба каталогів?

> ***Служба каталогів*** *(Directory Service) – це розподілена база даних з інформацією про мережеві об'єкти, а також засоби доступу до неї та підтримки.*

Вона дещо подібна до Реєстру (Registry) Windows 95, однак, на відміну від нього, містить параметри конфігурації не одного комп'ютера, а всіх об'єктів мережі. Наявність служби каталогів (СК) дає змогу створювати тільки один варіант реєстраційних параметрів кожного мережевого об'єкта. Наприклад, користувач, зареєстрований у СК, може працювати з багатосерверною мережею на будь-якій робочій станції і завжди працюватиме у звичному для себе середовищі. Без СК йому довелося б реєструватися на кожному сервері у випадку запуску кожного застосування. Аналогічні переваги СК має для централізованого збереження інформації про інші об'єкти мережі: файл-сервери, сервери друкування та принтери, модемні сервери тощо.

Запровадження СК дає змогу створювати та використовувати розподілену систему керування ресурсами мережі, перерозподіляти навантаження, оптимізувати надання послуг незалежно від місця розташування відповідних серверів та реально наблизитися до створення розподілених інформаційних систем.

Служба каталогів, як звичайно, зберігає бази даних про мережеві об'єкти у багатьох місцях (для зменшення часу доступу), інформація в різних копіях багаторазово продубльована для надійності (пор. з DNS, розділ 13).

Історично сформувалися два типи СК – ієрархічні (переважають на ринку, простіші в адмініструванні) та на базі доменної архітектури (каталоги мають пласку структуру, у якій кожен домен відображає конкретну групу серверів).

23.2. Історія розвитку служб каталогів

Розвиток служб каталогів значною мірою був зумовлений потребою вирішити проблеми усунення багаторазової реєстрації клієнта.

Спочатку була окрема мережева ОС. Клієнт, входячи у мережу, реєструвався на певному сервері. У цьому випадку перевірялися його повноваження та права доступу. Отже, клієнт був 'прикріплений' до цього сервера. Наприклад, у Novell Netware 3.11 інформація каталогу зберігалася в базі даних *bindery* кожного сервера. Кожен сервер мав свою базу і для роботи з іншим сервером потрібна була повторна реєстрація. Однак під час роботи з системою, що має велику кількість серверів, перереєстрація була незручною.

Наступним кроком став перехід до ієрархічних або доменних СК. У цьому випадку користувач реєструвався один раз у дереві каталогів або у визначеному домені. Ієрархічна структура виявилася зручнішою порівняно з доменною, і фірма Microsoft використовує її у Windows NT 5.0 (Active Directory). Після реєстрації користувач може працювати з усіма ресурсами дерева або домену. Таке вирішення дало змогу працювати в мережах однієї ОС. Залишилася проблема організації роботи гетерогенних систем.

Ще одну проблему – роботи в гетерогенних мережах – можна вирішити, максимально поширивши найпопулярніший продукт СК (наприклад, Novell безкоштовно або за мінімальну ціну продає свій продукт NDS, інтегрований у Unix або Windows NT), розробивши продукти-посередники, які забезпечують взаємодію різних СК (наприклад, продукт VIA фірми Zoomit) або використовуючи єдиний протокол доступу до каталогів (такий як LDAP або X.500). Історію розвитку конфігурацій СК описує рис. 23.1.

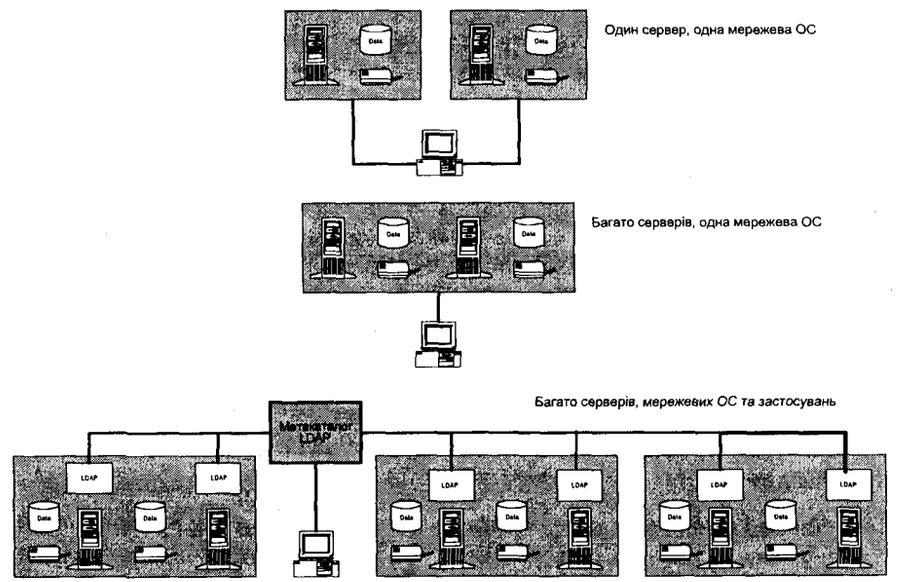


Рис. 23.1. Різні організації СК.

Як приклад однієї з найрозвиненіших служб каталогів розглянемо службу каталогів NDS, яка є частиною операційної системи Novell Netware 4.x а також і окремим продуктом.

23.3. Служба каталогів NDS

У основі архітектурної концепції Novell 4.x є **Служба каталогів Netware** (Netware Directory Services (**NDS**)). Згідно з цією концепцією всі ресурси мережі зображені об'єктами, занесеними в спеціальну розподілену базу даних – *Netware Directory Database*. Визначено різні можливі типи об'єктів: користувач, сервер, том, група користувачів та інші. Ці об'єкти згруповані в ієрархічному дереві. Ієрархічна деревоподібна структура відображає взаємну підпорядкованість об'єктів. Кожен об'єкт конкретного типу має власний набір властивостей та їхніх значень. Зокрема, об'єкт типу *користувач* має такі властивості: ім'я, пароль, поштову адресу, адресу електронної пошти, номер телефону, належність до груп користувачів тощо. Особа, яка працює в мережі, може аналізувати властивості об'єктів у NDS. Співвідношення понять *об'єкт*, *властивість*, *значення властивості* для об'єкта типу *користувач* показане на рис. 23.2.

Об'єкт	Властивість	Значення
Користувач	Ім'я	AKoval
	Телефон	255-1242
	Адреса електронної пошти	AKoval@icm

Рис. 23.2. Співвідношення понять *об'єкт-властивість-значення*.

NDS діє на базі структури об'єктів, яку називають **дерево каталогів** (Directory tree). Вона має три структурні типи об'єктів:

- кореневий об'єкт (Root);
- контейнерний об'єкт (Container object);
- кінцевий об'єкт (Leaf object).

Кожне дерево має тільки **один кореневий об'єкт**. Йому умовно відповідає об'єкт – увесь світ. Контейнерні містять інші об'єкти. Кінцеві об'єкти є головними, з якими працюють.

Приклад дерева каталогів показано на рис. 23.3.

Контейнерні об'єкти, як уже зазначено, містять інші об'єкти. Вони призначені для організації та групування кінцевих об'єктів. Визначені такі типи контейнерних об'єктів:

- **C – Країна** (Country) – містить код позначення країни та не є обов'язковим. Кожне дерево може мати не більше одного рівня країн.
- **O – Організація** (Organization) – містить назву організації та є обов'язковим. Кожне дерево повинно мати не менше одного об'єкта цього типу. Однак допустимий тільки один структурний рівень об'єктів-організацій.

- **OU – Організаційний підрозділ** (Organizational Unit) – зберігає інформацію про певний підрозділ організації та його параметри. Об'єктів OU в дереві може бути довільна кількість, вони можуть бути довільним чином вкладені один в одний.

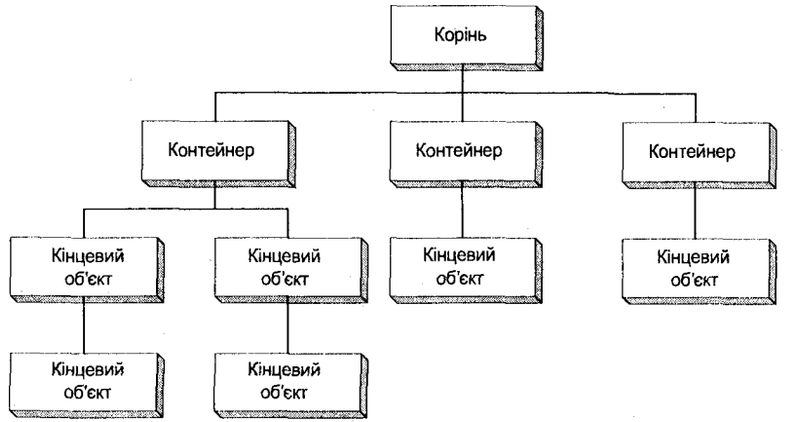


Рис. 23.3. Дерево каталогів.

Кінцеві об'єкти. Для кінцевих об'єктів використовують позначення **CN** (Common Name). Для зручності наведення кінцевих об'єктів згрупуємо їх відповідно до функціонального призначення. Визначено такі типи кінцевих об'єктів:

за технічним забезпеченням:

Netware Server	**Сервер**	Об'єкт зберігає інформацію про параметри сервера Netware
APF Server	**Сервер Macintosh**	
Computer	**Несерверний комп'ютер**	Цим комп'ютером може бути робоча станція мережі або маршрутизатор
Print server	**Сервер друкування**	
Printer	**Друкарський пристрій**	
Print queue	**Черга на друкування**	

за користувачами мережі:

User	**Користувач**	Містить дані про користувача
Group	**Група**	Об'єднує кількох користувачів та призначена для присвоєння їм певних повноважень
Organizational role	**Посада**	Для надання певних повноважень посаді, незалежно від особи, яка цю посаду обіймає

за елементами програмного забезпечення:

Volume	**Том**	Том на диску сервера. Він одночасно фігурує і в NDS, і в файловій системі, поєднуючи їх у єдине ціле
Directory map	**Відображення каталогу**	Використовують з метою полегшити шукання файлів
Profile	**Профайл**	Спеціальний командний файл, який створюють для групи користувачів
Alias	**Псевдонім**	Використовують для зображення цього об'єкта в конкретному місці дерева

об'єкти, введені для сумісності з Novell Netware 3.11:

Bindery	**База даних прив'язування до сервера**	База даних, у якій зберігається прикріплення користувача до конкретного сервера
Bindery queue	**Черга доступу**	

На рис. 23.4 показані приклади можливих структур дерев.

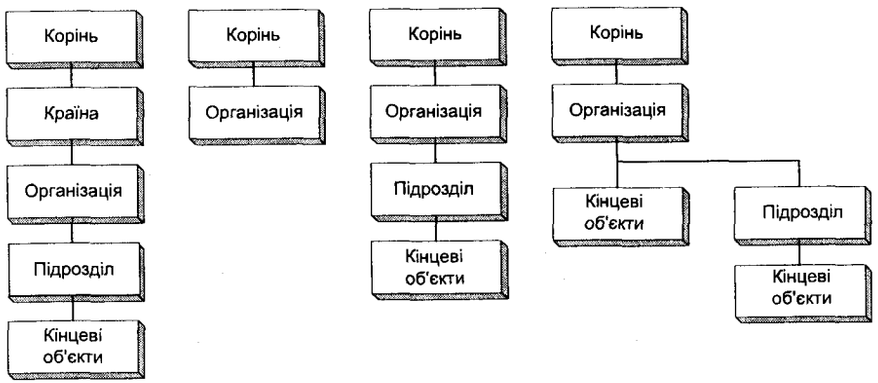


Рис. 23.4. Можливі структури дерева каталогів.

Зазначимо, що об'єктом NDS є не сам фізичний об'єкт (сервер або принтер), а лише інформація про нього, що зберігається у розподіленій базі даних.

Приклад дерева зображений на рис. 23.5.

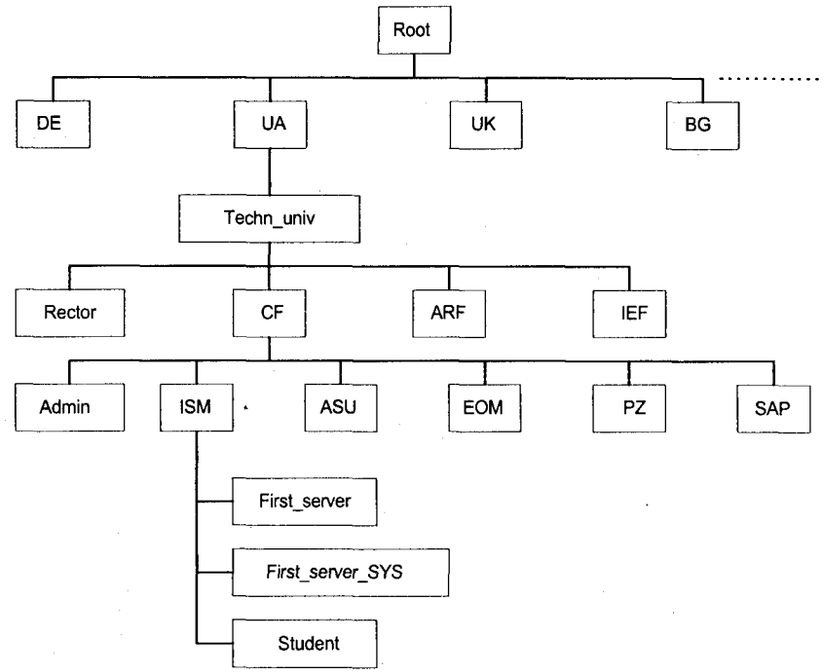


Рис. 23.5. Дерево каталогів.

Бібліографія та джерела

1. *Борисов В.* Сетевые службы Windows NT 5.0 // Компьютерпресс. 1998. № 10.
2. *Нортон Р., Помпили Т.* От сетевых ОС к сети // PC Magazine/RE. 1997. № 2.

Розділ 24

БЕЗПЕКА ДАНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Загальна характеристика та принципи організації системи безпеки. Таблиці правомірності. Біометрія. Розпізнавання. Використання брандмауерів та proxy-серверів. Рівні захисту інформаційних систем.

24.1. Загальна характеристика та принципи організації системи безпеки

Однією з головних проблем, що виникає під час проектування, встановлення та експлуатації комп'ютерної мережі, є безпека даних, оскільки перевагою мережі є доступ до спільних даних та пристроїв, а це зумовлює можливість несанкціонованого доступу до даних.

Головне право, яке визначає доступ до інформації, є 'право на таємницю', тобто *право окремої особи чи організації визначити як, коли і яка інформація може бути передана іншим.*

Отже, ***безпека даних*** *– це захист ресурсів мережі від руйнування та захист даних від випадкового чи навмисного розголошення, а також від неправомірних змін.*

Як бачимо, безпека даних не обмежується тільки захистом від несанкціонованого доступу, а передбачає також захист від збоїв та несправностей апаратного й програмного забезпечення, зовнішніх руйнівних чинників (пожежі, крадіжки тощо). Гарантувати безпеку даних покликаний адміністратор мережі. У великих мережах з цією метою передбачені спеціальні посади (security officers). Для гарантування безпеки даних розробляють багаторівневу систему захисту, що потребує таланту та винахідливості. Дуже часто потужна система захисту на практиці має слабкі місця, а це призводить до того, що її легко обійти (приклад – замок з укріпленнями та ровом: просто зробити підкоп або переліт). Приклад реалізації системи безпеки на рівні конкретних операційних систем див. у розділах 34, 35, 41, 43.

У сучасних системах захист даних реалізуюєть на багатьох рівнях (рис. 24.1):

- вбудовані засоби захисту – програмно-системні (паролі, права доступу та ін.);
- фізичні засоби захисту – замки, двері, охорона, сигналізація тощо;
- адміністративний контроль – організаційні заходи, накази адміністрації;
- законодавство та соціальне оточення – соціальний клімат колективу, нетерпимість до несанкціонованого використання чужої інформації, комп'ютерного 'піратства', закони про захист авторських та майнових прав.

Рис. 24.1. Рівні безпеки даних.

Можна виділити такі десять вимог до захисту даних.

Для користувачів
1. Користувачі, перш ніж розпочати роботу, повинні ідентифікувати себе.
2. Система повинна мати змогу контролювати дії користувачів.
3. Над діями користувачів потрібно вести постійний контроль – моніторинг – з метою виявлення неправомірних дій.

Для даних
4. Дані, апаратуру та програми потрібно захищати від пожежі, крадіжки та інших форм руйнування.
5. Дані, апаратура та програми повинні мати замки від несанкціонованого використання.
6. Дані повинні бути поновлювальними.
7. Дані повинні передбачати можливість ревізії. Завжди можна перевірити і довести їхню правильність.
8. Дані, апаратуру та програми потрібно захистити від зловмисників. Щоб найхитріший з них не зміг обійти систему захисту.

Для передавань інформації
9. Передавання захищають від помилок.
10. Передавання даних повинні бути конфіденційними. У випадку потреби їх шифрують.

У кожній інформаційній системі можна виділити найслабші з погляду безпеки місця. На них адміністратор повинен звернути увагу передусім. До таких місць, як звичайно, належать: сховища даних, адміністративна система, кабельна система, система доступу з зовнішніх мереж. Зловмисник, знайшовши доступ до сховища даних, зможе взяти з нього конфіденційні дані, а зайшовши в адміністративну систему, він матиме доступ до всіх ресурсів системи. До кабельної системи завдяки її розгалуженості легко приєднатися, підслухати та проаналізувати дані, що передаються, або підмінити їх іншими.

Долають труднощі, пов'язані з безпекою даних, одночасно у трьох напрямах:

- профілактика; мінімізація ймовірності настання небажаних подій; ліквідація можливостей несанкціонованого доступу; профілактика апаратури;

• якщо небажана подія сталася, система повинна бути побудована так, щоб мінімізувати шкоду, якої ця подія завдасть;

• створення процедур архівування та поновлення інформації у випадку її втрати.

Для прикладу розглянемо можливу послідовність дій та перевірок, які можуть траплятися у випадку налаштування сполучень.

Користувач вмикає комп'ютер.	Комп'ютер може бути фізично закритий на замок.
Користувач набирає номер або просить дозволу на сполучення.	Засоби зв'язку можуть мати замки або ж програмне забезпечення може не приймати запиту.
Мережевий рівень протоколу пробує налагодити сполучення.	Можна одержати відмову, якщо станція не належить до визначеної групи.
Сеансовий рівень протоколу пробує налагодити сеанс.	Програмне забезпечення на будь-якому кінці може відкинути запит про налагодження сеансу.
Користувач повідомляє своє ім'я.	Програмне забезпечення на прикладному рівні може не містити у своїх таблицях цього імені.
Користувач набирає пароль.	Пароль може виявитись неправильним.
Користувач звертається до програми.	Він може і не бути в списку осіб, допущених до роботи з програмою.
Рівень відображення містить шифрування для цього сполучення.	Станція може не мати засобів для дешифрування або ключів.
Програма відкриває файл і звертається до запису.	Програма або користувач можуть не мати права звертатися до цього файлу або запису.
Система читає запис і переглядає окремі поля.	З записами та окремими полями можуть бути пов'язані інші замки.
Програма опрацьовує дані та формує відповідь.	Відповідь та результати опрацювання можуть припинити подальші дії та заборонити передавання результату.
Передається відповідь.	

24.2. Таблиці правомірності

Як же на практиці відбувається надання та обмеження прав доступу? Найпростіше описати цей механізм з використанням **таблиць правомірностей**. Таблиця правомірності ставить у відповідність певній категорії об'єктів операційної системи права доступу до інформації (переглядання, читання, створення, записування тощо). Такими об'єктами можуть бути:

• окремі користувачі;
• *групи користувачів*;
• ступінь таємності;
• прикладні програми;
• час доби;
• робоча станція;
• довільна комбінація цих об'єктів.

Цей підхід дає змогу гнучко сформулювати складні обмеження доступу (наприклад, дозволити доступ до каталогу з ігровими програмами тільки на час обідньої перерви або з певних робочих станцій). Вислідні права доступу для користувача, які формуються як комбінація обмежень з таблиць правомірності, називаються *ефективними правами доступу* цього користувача.

24.3. Персональна ідентифікація

У деяких системах (наприклад, банківських чи податкових) потрібна ідентифікація не користувача, а фізичної особи. Розрізняють кілька способів такої ідентифікації.

1. **За персональними фізичними ознаками (біометрія)**. Знімають відбиток пальця, а потім аналізують. Інший спосіб: система пропонує повторити певну кількість випадково вибраних слів та аналізує особливості голосу. Такі системи діють досить надійно, однак дорогі.

2. **За предметом**, який особа-користувач носить з собою. Таким предметом може бути спеціальний значок, магнітна картка з кодом. Цей спосіб є дешевим, проте ненадійним, предмет можна підробити, вкрасти тощо.

3. **За тим, що особа повинна знати або пам'ятати**. Треба пам'ятати пароль або правильно відповісти на низку запитань. Цей метод найдешевший і найпоширеніший, але ненадійний (пароль можна підібрати, відповіді вгадати).

24.4. Розпізнавання

Важливим поняттям проблематики захисту даних у мережах є розпізнавання.

Розпізнавання *– це гарантування, що інформація (пакет) надійшла від законного джерела законному одержувачу.*

Справді, однією з найпоширеніших практик зловмисників у мережах є перехоплення пакетів та підміна їх своїми або скерування їх іншому адресату. Тому всі сучасні мережеві протоколи, як звичайно, оснащені засобами розпізнавання. Одним з механізмів розпізнавання пакетів є розміщення у відправника та одержувача однакових генераторів псевдовипадкових чисел. Кожен пакет позначають псевдовипадковим числом, яке порівнюється з таким же числом одержувача.

24.5. Захист мережі з використанням брандмауерів та серверів-посередників

Первинне значення терміна **брандмауер** (firewall) – це стіна у будівлі, зроблена з вогнетривких та незаймистих матеріалів, яка може перешкодити поширенню пожежі. У комп'ютерній мережі брандмауер – це комп'ютер з програмною системою, який ставлять на межі мережі і який перепускає тільки авторизовані певним чином пакети (рис. 24.2).

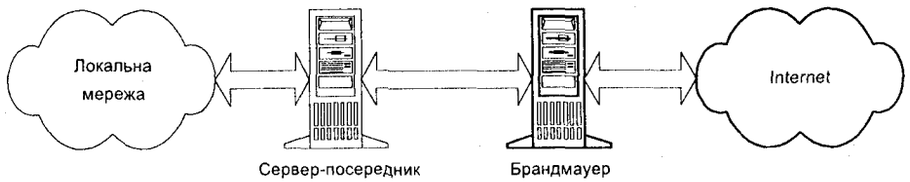


Рис. 24.2. Брандмауер та сервер-посередник.

Найчастіше брандмауери захищають внутрішню корпоративну мережу від зазіхань із зовнішньої мережі. Однак їх можна використовувати для фільтрування вихідної інформації, обмеження доступу користувачів внутрішньої мережі назовні.

Брандмауери застосовують різні алгоритми фільтрування, вони мають різні ступені захисту та вартість. З метою класифікації брандмауерів їхню роботу описують з використанням *семирівневої еталонної моделі взаємодії відкритих систем*.

Розрізняють:

- брандмауери з фільтруванням пакетів (packet filtering firewall; працюють на канальному, мережевому рівнях);
- шлюзи сеансового рівня (circuit level gateway; працюють на сеансовому рівні, розпізнають сеанс);
- шлюзи рівня застосувань (application level gateway; фільтрують інформацію за застосуваннями);
- брандмауери експертного рівня (stateful inspection farewall; виконують функції брандмауерів усіх нижніх рівнів).

Як звичайно, чим вищий рівень роботи брандмауера, тим більший рівень захисту, який він забезпечує, і тим більша його вартість.

Брандмауери з фільтруванням пакетів працюють разом з апаратним або програмним маршрутизатором. Вони аналізують зміст IP-заголовків пакетів і на підставі інформації у них та своєї таблиці правил приймають рішення про проходження пакета чи його відкидання.

Найчастіше інформацією, на підставі якої приймається рішення про проходження пакета, є його повна адресна інформація, тобто адреси відправника та одержувача, інформації про протокол та застосування, номери портів одержувача та відправника.

Рішення про перепускання пакета приймається у процесі аналізування таблиці правил брандмауера. Якщо пакет не задовольняє жодне з правил, то діє правило 'за замовчуванням'. Воно найчастіше відкидає пакет.

Конкретна конфігурація правил залежить від політики організації. Наприклад, можна заборонити вхід у мережу окремим комп'ютерам або обмежити вхідний потік тільки поштовими повідомленнями (на адресу сервера пошти) та ін.

Брандмауери з фільтруванням пакетів порівняно дешеві та генерують невелику затримку у передаванні повідомлень. Часто функції фільтрування пакетів інтегрують у маршрутизатори. Водночас рівень захисту у таких брандмауерів незначний – зловмисник може підмінити адресну частину IP-пакета.

Шлюзи сеансового рівня розпізнають учасників сеансу. Процедури перевірки виконують тільки на початку сеансу. Після того, як автентичність клієнта та сервера підтверджена, такий шлюз просто копіює пакети, не виконуючи фільтрування. Шлюзи сеансового рівня підтримують таблицю діючих сеансів і, коли сеанс завершується, знищують відповідний запис. Копіювання пакетів виконують спеціальні програми, які називаються *канальними посередниками (pipe proxies)*.

Шлюзи сеансового рівня, крім інших функцій, можуть виконувати і функцію **сервера-посередника**. Такий сервер відображає внутрішні адреси локальної мережі в одну (фактично адресу брандмауера). Для пакетів, що йдуть у зворотному напрямі, виконується зворотна операція. Отже, адресний простір мережі захищено – зовнішній користувач не бачить внутрішніх адрес.

Однак такі шлюзи не забезпечують достатнього захисту і тому, як звичайно, не є окремим продуктом, а їх постачають разом зі шлюзами рівня застосувань.

Шлюзи рівня застосувань. Шлюзи сеансового рівня працюють на рівні застосувань. Застосуванням відповідають спеціальні програми-посередники. Вони можуть виконувати фільтрування на рівні застосувань. Кожне застосування може мати свого посередника. На відміну від посередників у шлюзах сеансового рівня, посередники рівня застосувань аналізують пакети на рівні застосувань. Наприклад, посередник застосування *FTP* може заборонити використання команди *put* для заборони передавання інформації на свій сервер.

Брандмауери експертного рівня поєднують риси всіх попередніх систем. Вони виконують фільтрування пакетів на канальному рівні, розпізнають сеанс як шлюзи сеансового рівня і мають змогу аналізувати й фільтрувати пакети за ознаками рівня застосувань. На відміну від брандмауерів рівня застосувань, які фактично передають інформацію між двома розірваними ланками передавання *клієнт–шлюз* та *шлюз–зовнішній комп'ютер* і спричинюють значну затримку в передаванні інформації, брандмауери експертного рівня налагоджують пряме сполучення між розпізнаним клієнтом та сервером. Для фільтрування потоку використовують спеціальні шаблони, евристичні правила, порівняння зі зразками, інші методи з арсеналу експертних систем. (Тому ці системи й одержали назву брандмауерів експертного рівня). Брандмауери експертного рівня забезпечують найвищий рівень захисту та високі параметри продуктивності.

Проблема прозорості брандмауера. В ідеальному випадку брандмауер повинен бути прозорим (непомітним) для клієнтів мережі. Це означає, що він не спричинює суттєвої затримки в передаванні інформації, не вимагає від клієнтів спеціальної реєстрації на брандмауері, відокремленої від реєстрації користувача в мережевій ОС. На практиці вимога прозорості брандмауера тою чи іншою мірою порушується.

Сервери-посередники (proxy-server). Інколи функції брандмауера в складних системах розподілені між власне брандмауерами та серверами-посередниками. У чому ж різниця між цими серверами? Брандмауер традиційно захищає мережу від зовнішнього впливу. Він фільтрує кадри канального рівня, розпізнає сеанс, який відкриває зовнішній користувач. Сервер-посередник контролює та обмежує вихід внутрішнього користувача назовні, а також часто є його представником. Функції сервера-посередника такі:

- приховує адреси внутрішніх станцій, подаючи всю мережу назовні як один комп'ютер з адресою сервера;
- кешує популярні web-сторінки, файли, так що користувачі не змушені звертатися до зовнішньої мережі. Популярну інформацію сервер оновлює автоматично з визначеною періодичністю.

24.6. Рівні захисту інформаційних систем

Міністерство оборони США у книзі "Критерії оцінки безпеки комп'ютерів" (Оранжева книга, названа так за кольором її обкладинки), визначає сім рівнів безпеки комп'ютерних та мережевих систем. Сьогодні ця розробка стала класичною і загальноприйнятою в усьому світі для класифікації ступеня захищеності системи.

В Оранжевій книзі визначені такі рівні безпеки:

- **D** – рівень мінімального захисту (Minimal Protection). Зарезервовано для систем, які одержали попередню оцінку, однак для класифікації за іншими рівнями не забезпечують потрібного рівня безпеки;
- **C1** – рівень вибіркової безпеки (Discretionary Protection). Дає змогу користувачам застосовувати обмеження доступу для захисту приватної інформації;
- **C2** – рівень керованого доступу (Controlled Access Protection). Містить вимоги рівня C1 плюс захист процесу реєстрації у системі, облік подій захисту, ізоляція ресурсів різних процесів;
- **B1** – рівень захисту за категоріями (Labeled Protection). До вимог рівня C2 додається можливість захисту окремих файлів, записів у файлах, інших об'єктів системи спеціальними позначками безпеки, що зберігаються разом з цими об'єктами. Вважається, що подолати такий захист може добре підготовлений хакер, а звичайний користувач – ні;
- **B2** – рівень структурованого захисту (Structured Protection). До вимог рівня B1 додається повний захист усіх ресурсів системи прямо чи непрямо доступних користувачу (пам'ять, процесор тощо). Вважається, що хакери не зможуть проникнути у систему з таким захистом;

- **B3** – рівень доменів безпеки (Security Domains). До вимог рівня B2 додається явна специфікація користувачів, яким заборонено доступ до певних ресурсів, повніша реєстрація потенційно небезпечних подій. Вважається, що навіть досвідчені програмісти не в стані подолати систему з таким рівнем безпеки;
- **A1** – рівень верифікованої розробки (Verified Design). Повний захист інформації. Специфіковані та верифіковані механізми безпеки. Вважається, що у систему з таким рівнем безпеки без дозволу не може проникнути ніхто (навіть спеціалісти спецслужб, таких як Агентство Національної Безпеки).

Бібліографія та джерела

1. Брандмауэры, или запирайте вашу дверь // Сети. 1997. № 2.
2. *Галатенко В.* Информационная безопасность: обзор основных положений // Компьютерное обозрение. 1996. № 33.
3. *Карве А.* Proxy-серверы стоят на страже // LAN Magazine. 1997. № 2.
4. *Мартин Д.* Вычислительные сети и распределенная обработка данных. Программное обеспечение, методы и архитектура: В 2 т. М.: Финансы и статистика, 1985.
5. *Мафтик С.* Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
6. Миф С2 развеивается // Compurterworld-Киев. 1996. № 39.
7. *Стенг Д., Мун С.* Секреты безопасности сетей. К.: Диалектика, 1995.

ДОДАТОК ДО РОЗДІЛУ 24

Д. 24.1. Деякі іншомовні терміни з проблематики безпеки даних

З часу виникнення комп'ютерних мереж виробилася певна термінологія, що описує явища та дії, які виконують як у випадку порушень безпеки, так і для боротьби з ними. Як звичано, ці терміни виникли англійською мовою і для відображення їх в українській літературі відповідних термінів нема або ж використовують мовні 'кальки'. Наведемо найважливіші терміни.

Англійський варіант	Український варіант	Пояснення
Cracker	Крекер	Особа, що проникає в мережу з ворожими намірами
Hacker	Хакер	Особа, що проникає в мережу без ворожих намірів, найчастіше з амбітних або інтелектуальних мотивів
Brute force attack		Жорстка атака, бомбардування системи паролями, доки вона не зламається
Data diddling		Махінації з даними – несанкціонована зміна даних після їх уведення
Dumpster diving		'Порпання у смітнику' – шукання паролів та іншої суттєвої інформації серед 'сміття'
Entrapment		Заманювання у пастку – навмисне розміщення у системі різноманітних дефектів з метою спровокувати та викрити спроби порушення захисту
Logic bomb	Логічна бомба	Резидентна програма, що активізується після того, як відбудеться певна подія
Sniffer		Винюхувач – програма, що стежить за трафіком у мережі
Spoofing		Надсилання електронної пошти від імені іншої особи
Tiger team		Група експертів, найнята організацією для злому її системи безпеки з метою виявлення слабких місць
Trap door		Секретні двері – прихований механізм, використання якого дає змогу обійти механізми захисту
Trojan horse	Троянський кінь	Довільна програма, яка, крім прямих дій, виконує й інші, прямо не пов'язані з головною функцією програми

РОЗПОДІЛЕНІ АРХІТЕКТУРИ МЕРЕЖЕВИХ ОБЧИСЛЕНЬ

Розділ 25

Історія розвитку архітектур обчислень у КМ. Централізовані пакетні обчислення. Модель з розподілом часу. Архітектура 'клієнт–сервер'. Системи з файловим сервером. Моделі: інтелектуального клієнта, інтелектуального сервера, розподіленої функціональної логіки, розподілених послуг. Розподілена однорангова модель. Об'єктні архітектури розподілених обчислень. Архітектура OMA. Архітектура DCOM. Технологія Java.

Розвиток архітектур мережевих обчислень дав змогу історично виділити кілька типів архітектур, що відображали рівень розвитку комп'ютерної науки і техніки своєї епохи та переважали у цей час.

25.1. Централізовані пакетні обчислення

У 70–80-ті роки головною моделлю організації обчислень була централізована пакетна (batch). Строго кажучи, її не можна вважати мережевою. Завдання перед виконанням готували на машинних носіях (перфокартах, перфострічках). З різних завдань формували пакет, який і виконувала машина. Посередниками між користувачами та машиною були оператори ЕОМ, які приймали завдання, закладали їх у машину, видавали результати користувачам. Цикл виконання завдань був досить тривалим (декілька днів). Це було пов'язане з потребою підготувати завдання, перфокарти й проконтролювати їх. Перевагою таких централізованих обчислень була можливість централізованого керування ресурсами, захист інформації, можливість колективного використання великої ЕОМ багатьма користувачами. Водночас така модель обчислень мала і суттєві недоліки. Пакетний режим відділяв користувачів від комп'ютера, неможливо було виконувати оперативні задачі. Централізована архітектура була негнучка, а вартість машинного часу велика (на один-два порядки більше порівняно з моделлю обчислень 'клієнт–сервер').

25.2. Модель обчислень з розподілом часу

Модель централізованих обчислень застосовували переважно на великих ЕОМ. З появою у 80-ті роки міні-ЕОМ набула популярності модель обчислень з розподілом часу. Вона ґрунтувалася на тому, що до центральної ЕОМ приєднували неінтелектуальні алфавітно-цифрові термінали. Під час роботи кожному з терміналів виділявся певний процес комп'ютера (госта). Час центрального процесора був розподілений між процесами, що обслуговували термінали. Архі-

тектура з розподілом часу ЦП дала змогу безпосередньо наблизити користувачів до комп'ютера, реалізувала роботу в оперативному, діалоговому режимі і на цей час була значним кроком уперед. Водночас така архітектура мала і недоліки – примітивність та збідненість користувацького інтерфейсу, неможливість роботи з кількома гостями одночасно, недостатню гнучкість. Перехід на графічні X-термінали поліпшив інтерфейс, однак значно підвищив вартість системи. Незважаючи на колективний характер використання ресурсів, таку модель навряд чи можна вважати 'розподіленою'.

25.3. Архітектура обчислень 'клієнт–сервер'

Поява персональних комп'ютерів, розподіленого інтелекту та комп'ютерних мереж привела до розробки нових, ефективніших архітектур, що працювали вже в КМ. Серед них чільне місце посіла найпопулярніша сьогодні архітектура 'клієнт–сервер'. Вона спеціалізує комп'ютери, присвоюючи їм ролі

- **клієнта** (клієнт звертається до сервера за інформацією) та
- **сервера** (сервер обслуговує запити клієнтів).

У загальному випадку кожен клієнт може працювати з багатьма серверами, а сервер – з багатьма клієнтами одночасно.

У моделі обчислень 'клієнт–сервер' виділяють такі три компоненти:

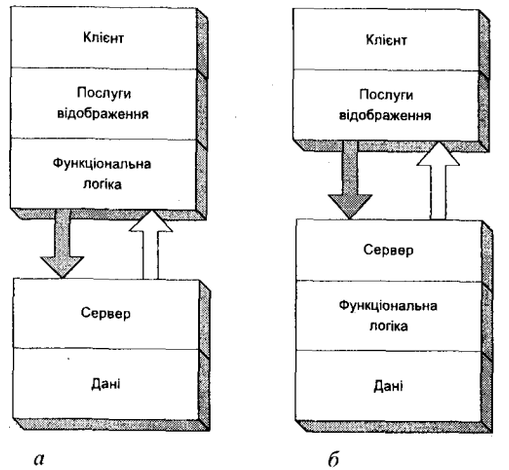
- **відображення**. Безпосередньо взаємодіє з користувачем, відображає інформацію, реалізує функції графічного інтерфейсу, формулює запит до сервера в узгодженому форматі;
- **логіки застосування (функціональної логіки)**. Відповідає за реалізацію ділових правил (Business rules), притаманних конкретному застосуванню. Виконує необхідні обчислення, порівняння, додаткові вибірки даних;
- **даних**. Відповідає за ефективну роботу з базою даних. Виконує вибірку або модифікацію даних, опрацювання даних згідно з командами.

Ці компоненти по-різному розподіляються між клієнтом та сервером, формуючи різні варіанти архітектури 'клієнт–сервер'.

Система з файловим сервером. У системі з файловим сервером опрацювання усієї інформації відбувається у клієнта. За запитом клієнта на його машину передається цілий файл. Файл-сервер оптимізовано власне для виконання файлових операцій. Архітектура з файловим сервером є в багатьох популярних системах, що надають файловий сервіс. Недоліком такої системи є те, що за запитом завжди передається весь файл, що перевантажує без потреби клієнта та мережу і недоцільне, особливо у системах, які працюють з базами даних (в інших системах файловий сервіс ефективніший). Системи файлового сервісу – це найпростіші та найменш розвинені системи архітектури 'клієнт–сервер'. Водночас наявність спеціалізованих на виконанні певних функцій серверів, універсальність клієнтів, можливість працювати з багатьма серверами дають підстави зачислити системи файлового сервісу до архітектури 'клієнт–сервер'.

Модель інтелектуального клієнта. У цій моделі компоненти відображення та логіки застосування реалізовані на клієнті, а компонента роботи з даними – на сервері (рис. 25.1,*а*).

Клієнт формує SQL-запити до сервера. Таку модель використовують для роботи невеликих систем підтримки робочих груп з 25–150 користувачами. Головна сфера застосування – підтримка прийняття рішень, а не виконання транзакцій. Модель інтелектуального клієнта реалізовано в таких продуктах, як Power Builder (Powersoft), SQL Windows (Gupta). Перевагами цих систем є використання потужностей клієнтів, розвантаження сервера. Недоліки випливають зі складності підтримки цілісності інформації та версій ПЗ на багатьох клієнтах, недостатня безпека даних, потрібні швидкісні ЛМ.



а *б*

Рис. 25.1. Моделі інтелектуального клієнта (*а*) та інтелектуального сервера (*б*).

У моделі інтелектуального сервера функціональна логіка повністю перенесена на сервер (рис. 25.1,*б*), фактично імітуються обчислення на головній ЕОМ. На таку систему ліпше переносити програми з великих ЕОМ, вона добре захищена, нею легше керувати. Функціональна логіка реалізована у вигляді процедур спільного використання. Тому зекономлено дисковий простір, час відповіді менший завдяки опрацюванню інформації на сервері. Глибина опрацювання інформації досить значна, тому мережею передається менше даних, ніж у системах моделі інтелектуального клієнта чи сервісу файлів. Водночас у випадку розширення системи потужності сервера стає замало. Недостатньо використані також потужності клієнтів.

Модель розподіленої функціональної логіки. У цій моделі компонента логіки застосування розділена між клієнтом та сервером (див. рис. 25.4,*а*). У процесі роботи застосування програми клієнта та сервера пов'язані між собою. Така система досить гнучка. Вона дає змогу динамічно переміщувати програми між клієнтом та сервером. Недоліком є тісний зв'язок клієнтів та серверів.

Архітектура розподілених мобільних обчислень. Звичайні системи архітектури 'клієнт–сервер' побудовані з використанням швидкісної локальної мережі, вони генерують інтенсивний

трафік обміну інформацією. Як звичайно, вони працюють з попереднім налагодженням сполучення з сервером (у сеансах). Мобільні системи, в яких комп'ютери приєднані за допомогою модема, відрізняються низькою швидкістю обміну з віддаленою системою, недостатньою надійністю зв'язку, частими його перериваннями. Під час роботи в архітектурі 'клієнт–сервер' з такими ненадійними каналами тривалість транзакції значно збільшується через процедури поновлення, перевірки тощо. Підвищити швидкодію роботи системи можна, зменшивши обсяг інформації, що передається ненадійним каналом, а також перейшовши у безсеансовий режим роботи.

Для підвищення швидкодії операцій з віддаленим сервером у випадку сполучення ненадійним та низькошвидкісним (найчастіше телефонним, комутованим, 'dial-up') каналом розроблена спеціальна архітектура обчислень. Суть її полягає у введенні, крім клієнтської програми, спеціальної програми 'агента', розташованого в одній локальній мережі з сервером (рис. 25.2).

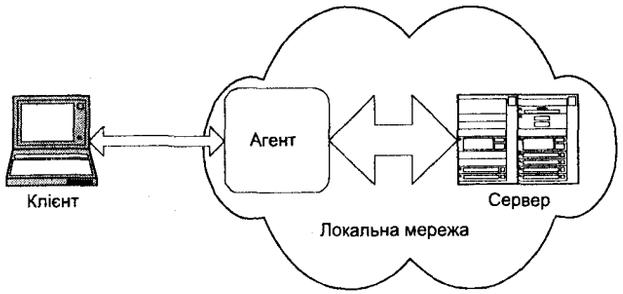


Рис. 25.2. Схема архітектури мобільних обчислень.

Агент є 'представником' застосування-клієнта у локальній мережі. Клієнт, як звичайно, надсилає агенту простий та короткий запит на виконання конкретної дії. Агент аналізує цей запит та організовує його виконання. У процесі виконання агент може неодноразово звертатися до різних ресурсів мережі. Готова відповідь на запит не обов'язково відразу ж передається клієнту. Якщо клієнт у якийсь момент недоступний, відповідь зберігає агент (можливо, з іншими відповідями) та передає її клієнту, якщо той приєднається до мережі (безсесійний характер роботи).

Розглянемо структуру системи на прикладі **Oracle Mobile Agents** (рис. 25.3).

На мобільному комп'ютері у загальному випадку кілька застосувань зв'язуються з сервером. У цьому разі вони звертаються до єдиної компоненти – *менеджера повідомлень*, який зв'язується з сервером одним з доступних у конкретний момент каналів (телефонним, локальної мережі тощо). Сполучення завжди відбувається з ініціативи користувача. У локальній мережі функцію одержання повідомлень та передавання відповідей сервера виконує *шлюз повідомлень*. Передавання інформації між менеджером повідомлень та шлюзом відбувається в асинхронному, безсесійному режимі. Це означає, що повідомлення можуть передаватися не відразу, а тоді, коли трапиться нагода. Кожне повідомлення є незалежною одиницею інформації.

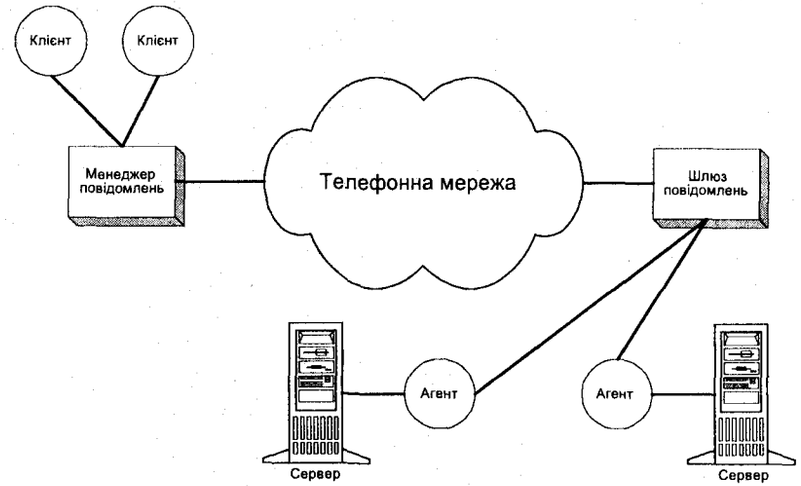


Рис. 25.3. Структурна схема роботи продукту Oracle Mobile Agents.

Модель розподілених послуг. Недоліком моделей архітектури 'клієнт–сервер' була недостатня спеціалізація серверів. У моделі розподілених послуг застосування є автономними та взаємодіють через мережу з використанням стандартних інтерфейсів (рис. 25.4,б). У цій моделі (її ще називають *трирівневою*) для підтримки функціональної логіки та даних призначені окремі сервери. Отже, сервер даних та сервер логіки можна оптимізувати для виконання

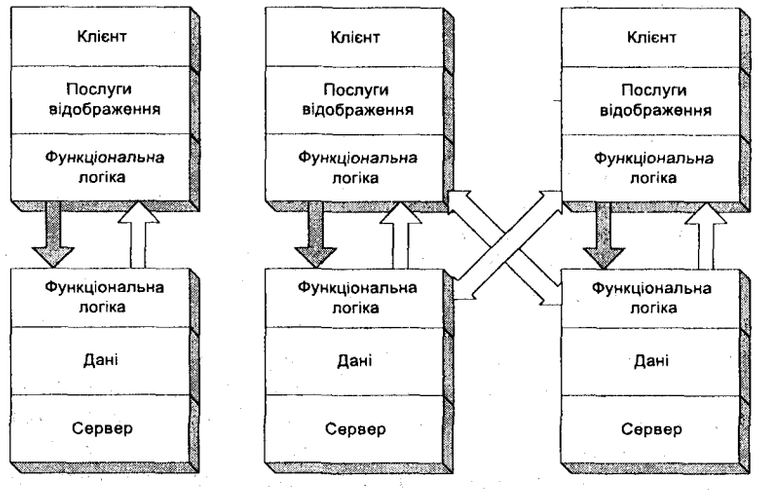


Рис. 25.4. Моделі розподіленої функціональної логіки (*а*) та розподілених послуг (*б*).

відповідних функцій. Наприклад, компоненту відображення розмістити на ПК, логічну – на сервері середнього рівня (Unix, Windows NT), а компоненту даних – на сервері верхнього рівня (Unix або мейнфрейм). Трирівнева модель історично була реалізована пізніше, ніж моделі інтелектуального сервера чи розподіленої функціональної логіки.

Модель розподілених послуг дає змогу стандартизувати процес надання послуг у мережі, раціонально використовувати програмні модулі, але потребує спеціалізованого проміжного інтелектуального ПЗ (middleware).

Розподілена однорангова модель. Модель розподілених послуг – це перший крок на шляху до розподіленої однорангової моделі. Згідно з нею все програмне забезпечення треба будувати як сукупність модулів, що взаємодіють один з одним через мережу з використанням стандартних інтерфейсів. Це дасть змогу багаторазово застосовувати модулі, виконати декомпозицію функцій у мережі, економніше використовувати ПЗ, зменшити його вартість. Складне завдання в цьому випадку вирішується в результаті взаємодії модулів.

Однорангову модель інтерпретують ще й як розподілені об'єктні обчислення. Незалежні програмні модулі є об'єктами, що об'єднують функції та дані і взаємодіють через стандартні інтерфейси. Об'єкт інкапсулює реалізацію функцій. Власне в об'єктній моделі знайшла логічне довершення архітектура 'клієнт–сервер'. У такій моделі кожен об'єкт може бути клієнтом та сервером залежно від потреби. Архітектури мережевих обчислень, що реалізують об'єктну модель – це новий розділ науки про комп'ютерні мережі. Зараз його інтенсивно розвивають, тому розглянемо об'єктні обчислення окремо.

25.4. Об'єктні архітектури розподілених обчислень

За допомогою об'єктних архітектур учені намагаються вирішити проблему організації розподілених обчислень та розподілених програмних систем. Ці архітектури підтримують новий підхід до обчислень, який повинен мати суттєві переваги порівняно з наявними. Головні характеристики цього підходу такі.

• **Процес розв'язування задачі можна зобразити як взаємодію компонент (модулів, об'єктів) через стандартні інтерфейси**. Об'єкти можуть бути створені різними виробниками. Це дасть змогу сформувати ринок об'єктів.

• **Внутрішня реалізація об'єктів інкапсулюється**. Це дає змогу багаторазово використовувати ті ж самі об'єкти, створювати екземпляри об'єктів у пам'яті тільки тоді, коли вони потрібні, знищувати їх, коли потреби у них вже нема.

• **Звертання до локальних об'єктів, об'єктів, що містяться в одній машині, але в іншому процесі, та об'єктів, що містяться у процесі в іншій машині, однакове**. Це дає змогу розглядати інформаційну мережу як єдине середовище, єдиний комп'ютер.

• **Кожен об'єкт**, як звичайно, **має унікальний номер-ідентифікатор** (Universally Unique IDentifier (**UUID**), Globally Unique IDentifier (**GUID**)). Жодний інший об'єкт у тій чи іншій машині протягом усього часу не може мати такого ж ідентифікатора.

• Об'єкти можуть через один інтерфейс допускати різні реалізації тих самих функцій (**поліморфізм**). Це дає змогу, наприклад, одночасно підтримувати нові та застарілі версії програм.

• Об'єкти дають змогу **успадковувати** інтерфейси або реалізацію інших об'єктів.

Передвісником появи сучасних архітектур розподілених обчислень були роботи Фонду відкритих систем (Open Software Foundation (**OSF**)), який розробив та стандартизував технологію (Distributed Computing Environment (**DCE**)). Елементи технології були використані в найвідоміших об'єктних архітектурах CORBA і DCOM, що мають багато спільного. Крім архітектур, під час створення розподілених систем велике значення має технологія Java.

25.4.1. Архітектура CORBA

У 1989 р. зусиллями одинадцяти компаній була створена асоціація OMG (Object Management Group) для розробки об'єктного підходу до розробляння розподілених інформаційних систем. Результатом діяльності цієї асоціації була розробка **OMA** (Object Management Architecture) зі специфікаціями **CORBA** (Common Object Request Broker Archirecture), **COSS** (Common Object Services Specification), **CF** (Common Facilities).

Головною частиною OMA є CORBA. Перша версія CORBA з'явилася в жовтні 1991 р., а версія 2.0 – у грудні 1994 р.

Об'єктну модель CORBA автори назвали класичною, оскільки вона має всі головні риси – поліморфізм, спадковість інтерфейсу та реалізації. Об'єкти можуть відсилати та одержувати повідомлення і змінювати свій внутрішній стан. У моделі CORBA, як і в інших моделях, передбачено відокремлення інтерфейсу об'єкта від його реалізації.

Для доступу до віддалених серверів та для опису взаємодії об'єктів використовують мову опису інтерфейсів **IDL** (Interface Definition Language), створену з метою забезпечити можливість опису інтерфейсів об'єктів незалежно від мови реалізації об'єкта. IDL наближена до мови С. У процесі реалізації на базі ORB конкретних застосувань IDL-описи інтерфейсу транслюються у набори функцій доступу до ORB, які потім зв'язуються з виконавчим модулем. Поняття 'інтерфейс' для CORBA однозначно відповідає типу об'єкта (отже, об'єкти CORBA не підтримують множинності інтерфейсів, як COM).

У CORBA визначені такі типи даних: базові (знакові та беззнакові цілі, числа з рухомою комою, булевий, ланцюжок символів, байт – Octal) та складні (інтерфейс, структура, послідовність, об'єднання та масив).

Розглянемо структуру CORBA. У цій архітектурі ORB є посередником між клієнтами та серверами, що призначений забезпечити прозорість процесу взаємодії як для клієнта, так і для сервера. Запит повинен відбуватися як локальний незалежно від реального розташування сервера. CORBA визначає три компоненти: *клієнтський інтерфейс*, *інтерфейс реалізації об'єкта та ядро ORB* (рис. 25.5).

Клієнтський інтерфейс складається з трьох базових інтерфейсів: *IDL-stub*, *інтерфейс динамічного виклику (Dynamic Invocation)*, *інтерфейс сервісів (ORB services)*.

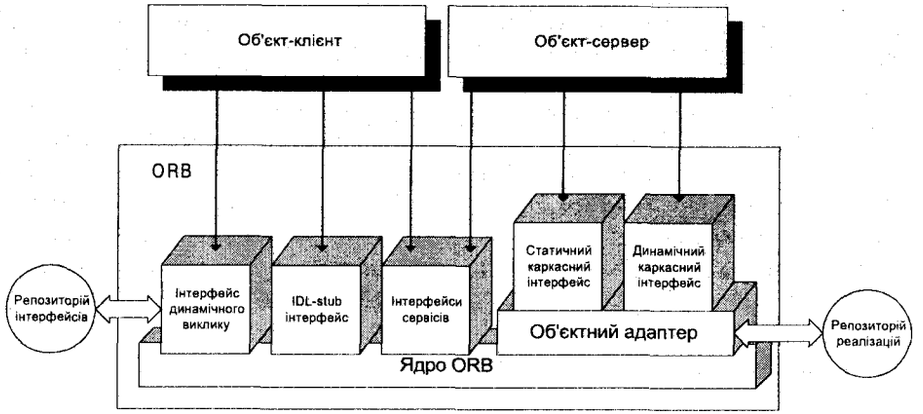


Рис. 25.5. Архітектура CORBA.

IDL-stub – це функції, згенеровані на базі IDL-визначень інтерфейсів та об'єднані з програмою. Спочатку їх пишуть мовою IDL, потім транслюють у мову програмування, якою створюють застосування. Отже, у випадку використання IDL-stub інтерфейсу програми клієнта взаємодіють з сервером, звертаючись до своїх локальних функцій.

Якщо інтерфейс, з яким буде працювати програма-клієнт, невідомий під час компіляції, то застосовується **інтерфейс динамічного виклику**. Він дає змогу робити запити до ORB з метою визначення інтерфейсів об'єктів. У запиті вказують тип потрібного об'єкта, тип запиту та параметри. Альтернативою є одержання інформації з репозиторію інтерфейсів. У цьому випадку треба зазначити унікальний ідентифікатор сервера (Universally Unique Identifier (UUID)).

Третім типом інтерфейсів, що доступні клієнту, є **інтерфейси сервісів**. Це набір функцій ORB, що доступні безпосередньо з програми-клієнта як для клієнта, так і для сервера. Інтерфейс IDL-stub забезпечує найшвидший доступ до сервера, а інтерфейс динамічного виклику є найгнучкіший.

Інтерфейс сервера має в основі *об'єктний адаптер (Object Adapter)*. Він доступний безпосередньо з сервера та обслуговує два типи інтерфейсів верхнього рівня:

- *статичний каркасний (Static Sceleton Interface)*;
- *динамічний каркасний (Dynamic Sceleton Interface)*.

Адаптер виконує такі функції: реєструє нові класи серверів, прототипи яких зберігаються в репозиторії реалізацій; створює робочі версії об'єктів-серверів за прототипами з репозиторію у випадку надходження запиту; призначає об'єктам унікальні ідентифікатори; повідомляє інші об'єкти про наявність зареєстрованого сервера; опрацьовує вхідні черги до серверів.

Статичний каркасний інтерфейс – це набір функцій, згенерованих з IDL-опису об'єкта-сервера, які викликає клієнт.

Динамічний каркасний інтерфейс дає змогу сполучатися з об'єктом-сервером під час запиту. Він перевіряє параметри, визначає адресу потрібного об'єкта та методу. Власне за

допомогою динамічного інтерфейсу можна створювати мости у передаванні повідомлень між кількома посередниками об'єктних запитів.

Ядро ORB для передавання повідомлень між брокерами використовує протокол **IIOP** (Internet Inter-ORB Protocol). Це версія протоколу TCP/IP з певним форматом поля повідомлення, яке дає змогу виконувати функцію посередника між посередниками. Формат повідомлення оптимізовано для відображення семантики міжоб'єктних повідомлень.

Крім CORBA, OMA описує також COSS та CF: COSS визначає набір серверів, що пропонують такі головні послуги, як підтримка циклів життєдіяльності об'єктів, генерація повідомлень, підтримка транзакцій, розпізнавання конфліктів; CF описує сервіси рівня застосувань, такі як друкування, електронна пошта, бази даних, складні документи.

25.4.2. Архітектура DCOM

Архітектуру **COM** (Component Object Model) та її варіант **DCOM** (Distributed COM) розробила фірма Microsoft. Історичним попередником цієї архітектури була OLE 1. Вона була зосереджена на документоцентричних застосуваннях, давала змогу вбудовувати документи різних застосувань один в одний. Архітектура OLE 2 розглядала загальнішу проблему *надання сервісів програмними компонентами для інших компонентів*. Тому в основі OLE 2 є COM. Сьогодні термін OLE використовують тільки для технологій пов'язаних документів, а для технології на базі COM використовують термін ActiveX.

Об'єкти COM діють у деякому середовищі, яке їх створює, контролює під час роботи та знищує (сервер). Кожен об'єкт підтримує один або кілька інтерфейсів. Кожен інтерфейс складається з методів. Множинність інтерфейсів дає змогу підтримувати старі та нові версії, групувати функції тощо (CORBA, наприклад, не допускає множинності інтерфесів. Для неї інтерфейс – це тип об'єкта. Java ж реалізує множинність).

Об'єкт COM – це екземпляр класу. Його створюють на підставі звертання до бібліотеки COM, що містить прототипи всіх доступних класів. Бібліотека COM запускає сервер підтримки об'єкта, створює об'єкт. Після створення об'єкта звертання надходить уже безпосередньо до нього, його інтерфейсів (рис. 25.6).

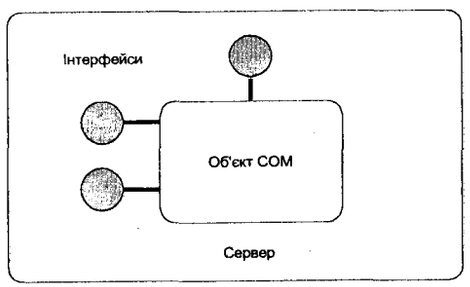


Рис. 25.6. Об'єкти COM, сервери та інтерфейси.

Об'єктність COM не повністю відповідає класичній моделі, реалізованій мовами програмування (однак COM – це не мова програмування). Класична модель характеризується інкапсуляцією коду, поліморфізмом та успадкуванням. Клас у COM – це прототип певного об'єкта, конкретна реалізація набору інтерфейсів. Може бути декілька різних реалізацій одного набору інтерфейсів, вони будуть різними класами. Можливість працювати з об'єктами різних класів, проте з однаковим інтерфейсом називається **поліморфізмом**.

Інкапсуляція – це відсутність прямого доступу до коду класу. Доступ до коду та параметрів виконується тільки через властивості об'єкта та методи. У COM доступ є тільки через визначені інтерфейси. Тому інкапсуляція підтримується повністю.

COM вирізняє два типи успадкування: успадкування реалізації та успадкування інтерфейсу. У випадку першого типу успадковується код батька. Це означає, що під час створення об'єкта формуються також і всі батьківські об'єкти. У COM реалізовано лише успадкування інтерфейсу. Об'єкт успадковує тільки визначення методів батька та підтримує їх. Це полегшує реалізацію поліморфізму.

> *Справді, успадкування реалізації у випадку взаємодії об'єктів передбачає два різні шляхи створення об'єктів: успадкування та прямий виклик. Крім того, успадкування реалізації менш гнучке, – якщо реалізація одного з батьків змінилася, потрібна підтримка як старої, так і нової реалізації. Взаємодія об'єктів допускає також множинний та умовний вибори об'єктів взаємодії. Взаємодія об'єктів може діяти в умовах неповної визначеності та неоднозначності вибору.*

Повторне використання коду у COM реалізується через механізми **включення** (containment) та **агрегування** (aggregation). Унаслідок включення один об'єкт викликає інший у міру потреби для виконання своїх функцій. У випадку агрегування об'єкт зображає один або кілька інтерфейсів іншого об'єкта як свої власні.

Створюючи архітектуру COM, розробники намагалися з'ясувати причини відставання розвитку програмних систем порівняно з розвитком обладнання. Серед головних причин вони назвали відсутність ринку програмних компонент. Їх виготовляють різні виробники для виконання спеціалізованих функцій. Компоненти можна якісно тестувати та використовувати багаторазово. Це дає змогу здешевити ПЗ. Однак підходи, що є сьогодні й орієнтовані на багаторазове використання ПЗ, недостатні, оскільки:

• **бібліотеки** хоч і не залежать від мови програмування, проте складні в розширенні та запровадженні нових версій.

• **об'єкти** повторно використовують на рівні робочих груп. Застосовувати їх ширше не можна з таких причин:

– немає стандартів для компонування двійкових об'єктів у єдине ціле (тому Java використовує інтерпретатор). Об'єкти, що взаємодіють, повинні бути скомпільовані одним компілятором. Тому наявні бібліотеки об'єктів C++ розповсюджують разом з початковими текстами. Породжені об'єкти тісно пов'язані з батьківськими. Автор породженого методу повинен мати доступ до тексту батьківського методу. Однак автори не зацікавлені у розповсюдженні початкових текстів;

– наявні різні об'єктні мови та середовища проектування;

– якщо змінюється один з об'єктів застосування, це потребує перекомпіляції всього застосування.

Усі ці проблеми дало змогу вирішити COM. За допомогою COM можна зручно структурувати сервіси. Проект визначається як сукупність об'єктів, після цього визначаються інтерфейси кожного об'єкта. COM зменшує різницю між системним програмним забезпеченням та застосуваннями. Звертання до всього ПЗ виконується однаково. COM не зважає на мову програмування. Важливим є тільки визначений двійковий інтерфейс. COM дає змогу контролювати версії. Старі інтерфейси не змінюються (COM це забороняє). Нові можливості реалізуються через новий інтерфейс.

Головні технології COM такі.

Автоматизація – це забезпечення можливості програмування застосувань. Інші програми можуть звертатися через визначені інтерфейси до сервісів застосування та одержувати результат.

Перманентність (persistency) – це здатність об'єкта запам'ятовувати свої дані на диску. Одним із способів, який застосовує COM, є структуроване сховище. Воно дає змогу багатьом об'єктам використовувати один файл. Внутрішня структура такого файлу деревоподібна та нагадує каталог з підкаталогами. У проміжних вершинах розташовані сховища, а в кінцевих – потоки (рис. 25.7).

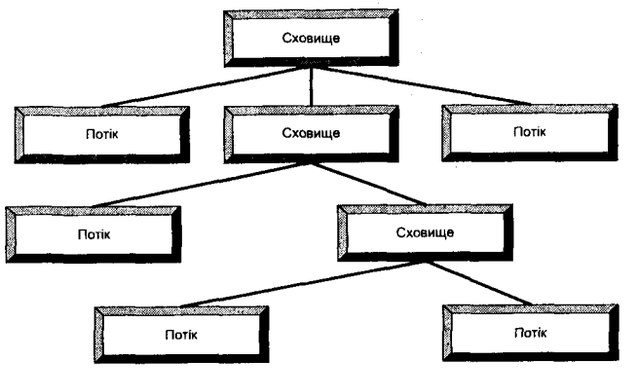


Рис. 25.7. Структуроване сховище.

Крім структурованого сховища, можливе збереження даних і у звичайному файлі чи у форматі WWW.

Монікери – це COM-об'єкти, призначені для створення та ініціалізації екземпляра іншого об'єкта.

Складні документи. Один з документів є контейнером, що містить файли інших застосувань у сховищі даних.

Розподілена COM. Для звертання до віддаленого сервісу DCOM використовує визначений у DCE виклик віддаленої процедури **RPC** (Remote Procedure Call). У DCOM також є засоби контролю доступу.

25.4.3. Технологія Java

Java – це технологія, реалізована спеціально для мережецентричних обчислень. Вона функціонує, дотримуючись клієнт-серверного підходу. Головна інформація зберігається на сервері. До клієнта мережею передаються тільки блоки, що потрібні у конкретний момент. Отже, все програмне забезпечення зберігається на сервері, який розповсюджує його.

Java найперше вирішує завдання з виконання програм на довільній платформі. Вона дає змогу створити програму один раз і використовувати її на різних платформах. Водночас доступ з Java-програми до програм на інших платформах ускладнений (непрозорий, можливий тільки шляхом реалізації виклику віддалених методів **RMI** (Remote Method Invocation)). CORBA ж дає змогу викликати процедуру, незважаючи на її розташування, однак реалізація об'єктів CORBA залежить від платформи.

Головна компонента Java – це віртуальний Java-процесор, який є спеціальним середовищем для виконання та інтерпретації Java-коду. Довільна Java-програма повинна відповідати специфікації віртуального процесора.

Головні функції технології Java реалізують такі компоненти:

- віртуальний процесор, який постійно контролює свій стан;
- завантажувач аплетів та програм (Class Loader), який контролює коди;
- диспетчер безпеки (Security Manager), який контролює та блокує всі потенційно небезпечні дії аплетів.

Необов'язковий елемент технології Java – мова програмування Java, оскільки є компілятори з інших мов (Ада), які дають змогу створювати байт-код Java.

Байт-коди Java спроектовані з метою максимального скорочення довжини команди. Java-процесор має мінімум регістрів, стекову архітектуру, часто використовує непряму адресацію. Середня довжина Java-команди – 1.8 байта. З використанням технології Java можна створювати програми довільної складності, однак головне призначення цієї технології – це створення невеликих програм (аплетів) для роботи в Internet. Мова Java наближена до C, за винятком функцій керування пам'яттю та вказівників. Java-програму, записану у проміжному байт-коді, інтерпретує спеціальний інтерпретатор. Байтові команди Java подібні до асемблерних. Швидкість виконання на порядок менша, ніж двійкової програми. Довжина коду Java не набагато менша, ніж двійкового коду.

Перевагою (та слабкістю) Java-технології є засоби захисту. Функції захисту виконують і віртуальний процесор, і завантажувач класу, і диспетчер безпеки. Завантажувач перепускає всі байтові коди через верифікатор. Код перевіряється на наявність багатьох нештатних ситуацій: переповнення стеків, доступ до недійсних регістрів, параметри функцій, правильність перетворення даних. Під час завантаження аплета у пам'ять йому виділяється власний простір імен та пам'яті. Різні аплети, завантажені від різних джерел, не можуть взаємодіяти. Не можна використовувати файлову систему клієнта (у деяких реалізаціях – тільки файли, розміщені у спеціальному списку користувача), створювати системні змінні, відкривати нові вікна без повідомлення користувача, виходити з інтерпретатора, одержувати доступ до іншого аплета.

Водночас такі заходи захисту Java утруднюють роботу розробників. Це особливо стосується взаємодії з ОС клієнта та його файловою системою, взаємодії аплетів. Вийти з цієї ситуації можна, сумістивши програмування мовою Java з програмуванням C++. Специфікація Java допускає це, незважаючи на те, що порушується 'чистота' мови. Аплети Java не захищені від декодування та копіювання. Java в певному сенсі полегшує декодування.

З технічного погляду Java не є брокером запитів до об'єктів, хоч і підтримує деякі функції ORB. Специфікація RMI є в зародковому стані. Вона підтримує одну мову програмування – Java. Для реалізації розподілених обчислень програми Java використовують архітектуру OMA та взаємодіють з DCOM.

Бібліографія та джерела

1. *Алексеенко М.М.* Mobile agents – новый продукт фирмы Oracle // СУБД. 1995. № 4.
2. *Васкевич Д.* Стратегия клиент-сервер. К.:, Диалектика, 1996.
3. *Коржов В.* Безопасность Java: миф или реальность? // Сети. 1997. № 2.
4. *Ричардсон Р.* Java под парами // LAN Magazine. 1996. № 4.
5. *Ричардсон Р.* В сетях OLE // LAN Magazine. 1996.№ 5.
6. *Сешнс Р.* Распределенные объекты // LAN Magazine. 1997. № 2.
7. *Слайва К., Мессмер Е.* Написав Java-апплеты один раз, можно выполнять их на чем угодно? Отнюдь! // Сети. 1997. № 3.
8. *Чеппел Д.* Технологии ActiveX и OLE. М.: Microsoft Press. Русская редакция, 1997.
9. *Юткин А.* Объектные технологии в распределенных системах // Открытые системы. 1995. № 3.
10. *Эккерсон В.* В поисках лучшей архитектуры клиент–сервер // Сети. 1995. № 4.

Розділ 26

БЕЗПРОВОДОВІ КОМП'ЮТЕРНІ МЕРЕЖІ

Загальна характеристика та сфери застосування. Класифікація безпроводових мереж. Мережі на радіомодемах. Технологія SST. Системи на базі інфрачервоних каналів. Мережі на стільникових модемах. Технологія CDMA. Технологія VSAT. Системи низькоорбітальних супутників. Радіорелейний зв'язок.

26.1. Загальна характеристика та сфери застосування

Останніми роками напрям безпроводових комп'ютерних мереж та віддаленого доступу зазнав бурхливого розвитку. Це пов'язано з поширенням блокнотних комп'ютерів, систем пошукового виклику (так званих пейджерів) та появою систем класу 'персональний секретар' (Personal Digital Assistant (PDA)). Такі системи повинні забезпечити ділове планування, розрахунок часу, зберігання документів та підтримку зв'язку з віддаленими станціями. Девізом цих систем стало 'anytime, anywhere', тобто надання послуг зв'язку незалежно від місця та часу. Крім того, безпроводові канали зв'язку актуальні там, де неможливе або дороге прокладання кабельних ліній та значні відстані.

Сьогодні більшість безпроводових комп'ютерних мереж передає дані зі швидкістю від 1.2 до 14.0 Кбіт/с, найчастіше вони передають тільки короткі повідомлення (передавання файлів великих розмірів чи довгі сеанси інтерактивної роботи з базою даних недоступні).

26.2. Класифікація безпроводових мереж

Залежно від технологій та передавальних середовищ, які використовують, можна визначити такі класи безпроводових мереж:

- мережі на радіомодемах;
- мережі на стільникових модемах;
- інфрачервоні системи;
- системи VSAT;
- системи з використанням низькоорбітальних супутників;
- системи з технологією SST;
- радіорелейні системи.

Федеральна комісія з електрозв'язку США (FCC) визначила такі категорії **PCS** (Personal Communication Services) та відповідні смуги частот:

- вузькосмугові PCS (діапазон 900–901, 930–931, 940–941 МГц) для високошвидкісних пейджерних мереж, двонапрямленого передавання повідомлень, передавання мовленнєвих повідомлень;

- широкосмугові PCS (120, 1850–2200 МГц); стільниковий зв'язок – цифрове передавання мовлення та даних.
- неліцензовані PCS (40 МГц, від 1890 до 1930 МГц) – безпроводові ЛМ та АТС організацій у найближчому радіусі дії – у межах одного будинку або групи будівель. Неліцензовані PCS забезпечують передавання даних зі швидкістю до 10 Мбіт/с.

26.3. Мережі на радіомодемах

Для передавання даних використовують смуги частот радіо та ультракороткохвильового діапазону. Кожен радіомодем має антену та передавач для напрямленого передавання сигналів. Як звичайно, швидкість передавання невелика, оскільки значний вплив завад. Замість радіомодемів щораз частіше використовують стільникові системи та системи SST, які забезпечують більшу перепускну здатність.

26.4. Технологія VSAT

Технологія **VSAT** (Very Small Aperture Terminal) використовує для передавання даних геостаціонарні супутники, розміщені над екватором Землі на висоті 40 тис. км. Наземні станції для зв'язку зі супутником застосовують еліптичні антени діаметром 3 м. Канал VSAT

- забезпечує швидкість передавання даних до 2 Мбіт/с;
- дає змогу реалізувати сполучення на великі відстані, з переходом державних кордонів;
- сумірний за ціною з кабельними каналами такої ж перепускної здатності.

Водночас цей канал відрізняється значними затримками передавання даних, зумовленими великою відстанню до супутника (затримка становить приблизно 250 мкс, тоді як для кабельних мереж – 15 мкс). Тому канал VSAT не можна використовувати у системах реального часу та оперативного зв'язку.

Оскільки вартість супутникового каналу велика, то фірма-провайдер послуг купує у власника супутника канал зв'язку великої ємності і продає частини перепускної здатності каналу. Отже, мережа з використанням ланок VSAT має зіркову структуру (рис. 26.1).

26.5. Системи низькоорбітальних супутників

Системи на базі низькоорбітальних супутників **LEO** (Low Earth Orbit), як і системи VSAT, для передавання використовують супутник. Однак супутник розміщено на висоті близько 100 км на звичайній, не геостаціонарній орбіті. У цьому випадку зменшується затримка в передаванні даних. Крім того, вивести такий супутник на орбіту значно дешевше, ніж геостаціонарний. Водночас для підтримування постійного зв'язку треба використовувати велику кількість таких низькоорбітальних супутників.

Серед наявних проектів LEO можна виділити систему **Iridium**, яка використовує 66 супутників.

У першому варіанті передбачалось, що в системі буде 77 супутників. Саме стільки електронів містить атом іридію. Пізніше виявилось, що достатньо буде 66. Однак назву вирішили залишити (елемент з 66 електронами диспрозій одержав назву від латинського disprosius – важкодосяжний).

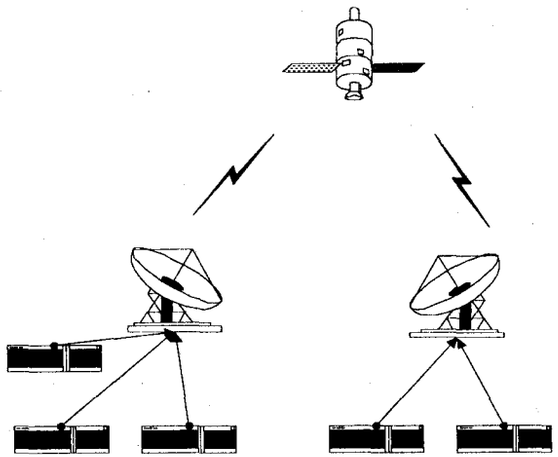


Рис. 26.1. Структура мережі VSAT.

Корпорація Teledesic, власниками якої є Bill Gates та Greg MacCaw, планує створити всесвітню систему передавання мультимедіа інформації на базі LEO-технології. Планується, що така мережа буде використовувати 840 супутників і надавати користувачам канали перепускної здатності від 62 Кбіт/с до 2 Мбіт/с.

26.6. Технологія SST

У технології **SST** (Spread Spectrum Technology) використано розподіл сигналу за спектром частот. Це дає змогу значно підвищити пропускну здатність каналу за рахунок більшої завадостійкості. Технологію SST уже тривалий час застосовували для військових потреб.

Є два різновиди мереж SST:

- FH-SS. Приймач та передавач синхронно перескакують з частоти на частоту;
- DH-SS. У кожний момент часу сигнал 'розмазано' по широкому діапазону частот.

Технологія SST дає змогу не тільки збільшити перепускну здатність мережі, але й ліпше реалізувати захист інформації від прослуховування. Зовнішній спостерігач таку інформацію сприймає як 'білий шум'.

26.7. Мережі на стільникових модемах

Мережі на стільникових модемах використовують наявну інфраструктуру стільникової телефонії. Вони працюють в особливо важких умовах великих завад, періодичного зникнення сигналу.

Ці технології можна розглядати згідно з протокольними рівнями. На фізичному та канальному рівнях визначають різноманітні методи доступу, які відображені у різноманітних технологіях.

З методів доступу виділяють аналогові, які використовують для передавання аналоговий сигнал. Це класичні методи доступу у стільникових мережах **FDMA** (Frequency Division Multiple Access), **TACS** (Total Access Communication System).

Головний ресурс стільникової мережі – це призначений для неї діапазон частот. Аналогові методи доступу виділяють для кожного передавання окремий канал – смугу частот у призначеному для мережі діапазоні. У цьому випадку сусідні стільникові комірки не можуть працювати в одному й тому ж діапазоні частот (інакше передавання в сусідніх комірках заважали б одне одному). Частотний діапазон поділяють на сім частин (рис. 26.2).

Серед методів доступу, які використовують цифрове передавання, популярні різні модифікації **TDMA** (Time Division Multiple Access). Вони застосовують відомий принцип розподілу часу передавання на окремі часові слоти. До цієї групи методів належать **AMPS** (Advanced Mobile Phone Service) (частотні канали завширшки 30 кГц поділяють на три часові слоти), **NAMPS** (Narrowband Advanced...), **PDC** (канали по 25 кГц, три слоти), **GSM** (діапазон 200 кГц, вісім слотів).

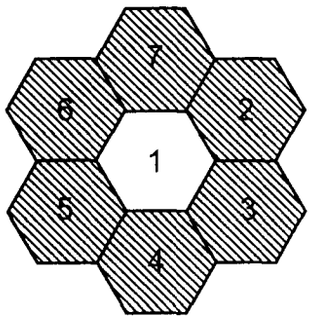


Рис.26.2. Комірки стільникової мережі.

Найбільш передовою сьогодні є технологія **CDMA** (Code Division Multiple Access), що використовує цифрове передавання. В основі CDMA є SST (DH-SS Direct Sequence Spread Spectrum) технологія передавання, коли інформація ніби 'розмазується' по широкому спектру частот. Послідовність інформаційних бітів множать на псевдовипадкову послідовність коротких імпульсів. Одержують сигнал, що є в ширшому частотному спектрі і має значно меншу інтенсивність. Для декодування такої послідовності треба знати псевдовипадкову послідовність, яку використовували під час передавання. Такий механізм кодування гарантує, що

- сигнал захищений від підслуховування. Треба знати псевдовипадкову послідовність-ключ. Це й пояснює широке використання цього підходу військовими;
- сигнал захищений від завад. Широкосмуговість сигналу дає змогу просто поновлювати сигнал, особливо, якщо завади вузькосмугові. Так само сигнал захищений і від тимчасового зникнення на окремих частотах (фейдинг – fading) (рис. 26.3);

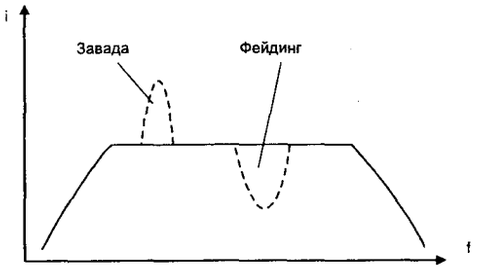


Рис. 26.3. Дія завад та фейдингів на широкосмуговий сигнал.

• широкосмугове передавання та ліпший захист від завад дають змогу зменшити потужність передавачів, збільшити час дії акумуляторів та дещо зменшити безперечно шкідливий вплив цієї технології на здоров'я людини;

• дві абонентські станції, які працюють у межах одної стільникової комірки на однаковій частоті з використанням різних кодувальних послідовностей, практично не створюють завад одна одній.

Тому для станцій, які працюють у межах однієї комірки, відведено спільний частотний діапазон завширшки 1.25 МГц, а також фрагменти спільної псевдовипадкової кодувальної послідовності (зі своїм зсувом від початку).

У мережі CDMA параметри розміру комірки, якості передавання та кількості каналів взаємозалежні. Наприклад, чим більше каналів у комірці, тим більше взаємних завад через неповну незалежність кодувальних послідовностей, тим гірша якість передавання. Чим більший розмір комірки, тим слабший корисний сигнал, тим меншим повинен бути рівень завад. Емпіричним шляхом визначено, що сьогодні в одному частотному діапазоні 1.25 МГц можна розмістити до 18 каналів для мобільних та 30 каналів для стаціонарних користувачів. Це майже у дев'ять разів більше, ніж у мережах AMPS.

Ще однією перевагою CDMA є змога використання у сусідніх комірках одного й того ж частотного діапазону, що полегшує планування мережі та збільшує кількість каналів.

Однією з особливостей, які поліпшують якість передавання у CDMA-мережах, є механізм відпрацювання переходу абонента з однієї комірки в іншу. В інших технологіях під час такого переходу спочатку розривається зв'язок з однією базовою станцією, а потім налагоджується з іншою (hard handoff, break before make). Це знижує якість передавання. У технології CDMA за рахунок збереження однієї частоти-носія у сусідніх комірках можна спочатку налагодити сполучення з новою станцією, а вже потім розірвати з попередньою. Це поліпшує якість переходу та дає змогу коректно опрацювати передавання у 'прикордонній зоні', коли передавач може багато разів переходити зі сфери діяльності однієї базової станції у сферу діяльності іншої та навпаки.

Мережі технології CDMA сьогодні активно впроваджують не тільки у традиційній сфері стільникового передавання, але й у частотному діапазоні PCS, виділеному для роботи як телефонів, так і іншого обладнання персонального зв'язку. Вони перевищують інші технології за якістю передавання та кількістю каналів. Наприклад, для CDMA потрібно на 30–40% менше базових станцій, ніж для аналогічних мереж GSM та у два-три рази менше станцій, ніж для мереж AMPS. Водночас вартість обладнання CDMA внаслідок його складності сьогодні вища, ніж аналогічного обладнання інших мереж.

На верхніх рівнях протоколу мережі передавання даних використовують спеціальні протоколи, орієнтовані на стільникову мережу.

Технологія **CDPD** (Cellular Digital Packet Data) реалізує як пакетне передавання (протокол TCP/IP), так і модемний інтерфейс (AT-команди). На відміну від радіомодемів стільникові модеми не використовують спеціальних антен та приймачів-передавачів, а відповідні пристрої стільникового телефону.

Під час передавання даних застосовують протоколи MNP-10 або ETC. Протокол MNP-10 динамічно оптимізує швидкість передавання даних та рівень сигналу, має розвинуті засоби опрацювання помилок.

Протокол ETC запропонувала у 1993 р. фірма AT&T Paradyne. Він базується на стандарті V.32bis (14.4 Кбіт/с). ETC дає змогу підтримувати зв'язок з іншими модемами стандарту ETC та іншими протоколами. ETC порівняно з MNP-10 більш досконалий технічно.

26.8. Системи на базі інфрачервоних каналів

Системи на базі інфрачервоних каналів відрізняються невеликою вартістю приймачів та передавачів (від 1.5 до 4.5$), високими швидкостями передавання. Однак інфрачервоні канали працюють тільки в умовах прямої видимості. Асоціація **Infrared Data Communications** розробила стандарт передавання інфрачервоним каналом зі швидкістю 115.2 Кбіт/с.

26.9. Радіорелейний зв'язок

Радіорелейні станції (РРС) використовують для передавання аналогового сигналу в телебаченні та цифрового в послідовному коді за стандартом ITU G.703 в телефонії. Канал G.703 має перепускну здатність 2 Мбіт/с. Його можна використати, наприклад, для сполучення сегментів Ethernet.

Сучасні цифрові РРС мають смугу перепускання 2–34 Мбіт/с. Тому часто її розділяють на декілька каналів. Максимальна відстань для зв'язку РРС – 60–80 км. Для наземних РРС використовують частотні діапазони 1, 5, 7, 15 ,23, 34 ГГц. Взаємодії маршрутизатора та РРС досягають за допомогою конвертера V.35/G.703.

Бібліографія та джерела

1. *Бродски И.* Будущее систем беспроводной связи // Сети. 1995. № 4.
2. *Йенсен Е.* Услуги распределенных сетей беспроводной связи // Сети. 1994. № 4.
3. *Крейг, М. Райсевич П.* Азбука персональных коммуникационных услуг // Сети. 1995. № 3.
4. *Крейнес А.* Код с правом передачи // Сети. 1997. № 7.
5. *Сатовский Б.* Использование радиорелейных систем связи в корпоративных сетях//Сети. 1995. №4.

МЕРЕЖІ X.25 ТА FRAME RELAY

Мережа X.25. Загальна характеристика та історія розвитку. Структура мережі. Протоколи та порядок передавання даних. Керування доступом. Засоби приєднання до мережі X.25 та відповідні стандарти. Мережа Frame Relay. Її протокольні рівні. Організація передавання даних. Порівняння з технологією X.25.

27.1. Мережа X.25

Загальна характеристика та історія розвитку. Мережі, що відповідають стандарту ITU X.25, почали розробляти в 70-х роках. Сьогодні вони досить поширені. Це типові мережі з налагодженням віртуальних сполучень та комутацією пакетів. Вони, поряд з новими типами мереж (Frame Relay, ATM), надають своїм клієнтам певний сервіс передавання даних. Топологічна структура мережі така (рис. 27.1): це багатовузлова мережа з вузлами комутації (ВК) пакетів та терміналами (див. розділ 1). Такими терміналами можуть бути як алфавітно-цифрові та графічні термінали, так і комп'ютери. У термінології мереж X.25 термінали називаються DTE, а вузли комутації – DCE.

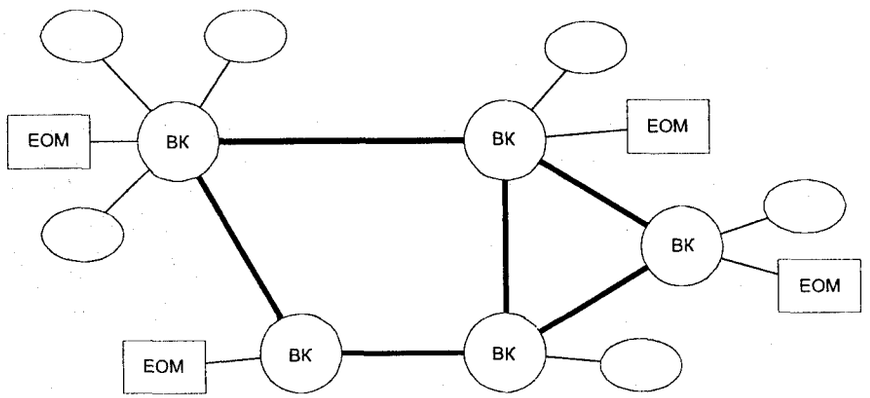


Рис. 27.1. Топологічна структура мережі X.25.

Мережі X.25 розробляли у період дуже ненадійних каналів зв'язку. Тому складовою таких мереж є суворі процедури виправлення помилок. Зокрема, кожен вузол мережі перевіряє коректність передавання та виконує коректувальні дії, проте внаслідок виконання таких дій зменшується вислідна швидкість передавання.

Протоколи та порядок передавання даних. Мережа X.25 – це глобальна мережа з віртуальними каналами. Віртуальний канал (віртуальний виклик, див. розділ 9) налагоджується між двома терміналами. Пакети одного каналу завджи йдуть одним і тим же маршрутом, в однаковій послідовності. Під час налагодження сполучення термінал, що викликає, вибирає з множини вільних номерів один та присвоює його віртуальному каналу. Термінал, що одержує, також вибирає один з вільних номерів логічного каналу. Мережа перетворює ці два номери в один унікальний для мережі, який ідентифікує віртуальний канал.

Порядок налагодження сполучення показано на рис. 27.2. Як бачимо, спочатку надсилається пакет налагодження сполучення. Він проходить через усю мережу. Після того, як підтвердження повернулося, віртуальний канал сформовано. Пакет відмови від сполучення підтвердження не потребує.

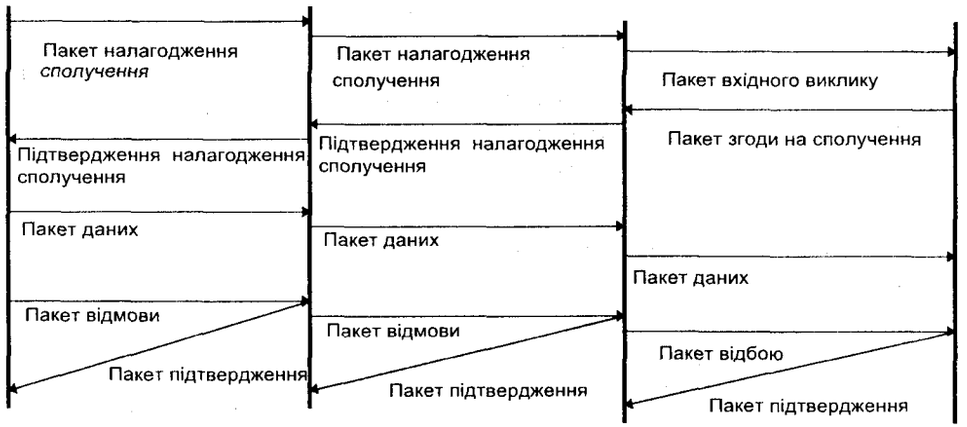


Рис. 27.2. Сеанс зв'язку мережі X.25.

Мережі протоколу X.25 можуть передавати і пакети інших мереж (наприклад, IP-пакети), розміщуючи їх у своїх пакетах. У цьому випадку великий пакет розділяють на фрагменти або об'єднують менші за розмірами пакети. У першому байті пакета налагодження сеансу (Call Set Up) зазначають ідентифікатор протоколу мережевого рівня.

Інкапсуляція пакетів може бути двох типів:

• SNAP-інкапсуляція. Кожен віртуальний канал може передавати тільки один тип пакетів протоколів (найчастіше – IPX- та OSI-пакети);

• нуль-інкапсуляція. Реалізують, якщо через один канал треба передавати пакети різних типів протоколів. Інформація про тип пакета передається з кожним пакетом.

Сама мережа X.25 підтримує три рівні протоколів, що в цілому відповідають трьом нижнім рівням еталонної моделі взаємодії відкритих систем (рис. 27.3).

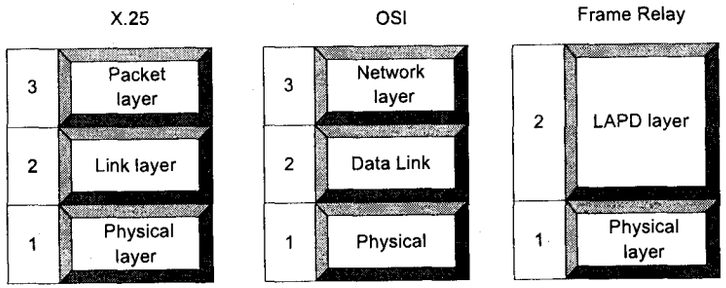


Рис. 27.3. Порівняння протокольних рівнів X.25 та Frame Relay.

Керування доступом. Стандарт X.25 дає змогу створювати так звані *закриті групи користувачів (Closed User Group (CUG))*. Для кожної такої групи можна:

- дозволити/заборонити доступ абонентів інших груп;
- дозволити/заборонити доступ абонентів цієї групи.

Розглянемо такий приклад (рис. 27.4). У мережі X.25 визначено п'ять користувачів dte (a, b, c, d, e), що належать до двох груп так, як це показано на рис. 27.4.

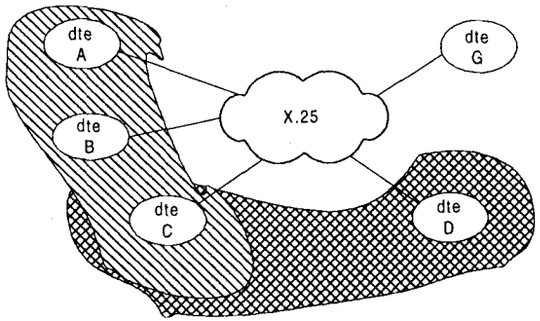


Рис. 27.4. Приклад обмеження доступу.

Обмеження доступу для визначених dte наведені у табл. 27.1.

Таблиця 27.1. Обмеження доступу для груп

Dte	Група	Обмеження доступу
A	1	Заборонено вихідні сполучення за межі своєї групи
B	1	Дозволено вхідні зовнішні сполучення, заборонено вихідні сполучення з членами групи 2
C	1, 2	Дозволено тільки вхідні сполучення
D	2	Дозволено вихідні сполучення тільки з членами групи 1, всі вхідні сполучення
G		

Вислідні права різних dte відображено у табл. 27.2.

Таблиця 27.2. Вислідні права різних dte

dte	Може передати інформацію	Може одержати інформацію від
A	B, C	B, C, D, G
B	A, G	A, C, D, G
C	A, B, C	A, B, D, G
D	A, B, C, D	A, B, C, G
G		A, B, C, D

Засоби приєднання до мережі X.25 та відповідні стандарти. Усі термінали, які приєднують до мережі X.25, поділяють на термінали, виконані з дотриманням вимог стандарту X.25 та інші. Якщо в першому випадку порядок приєднання тривіальний, то для приєднання не X.25 терміналів потрібні спеціальні пристрої – протокольні конвертери. Кілька терміналів приєднують до одного конвертера **PAD** (Packet Assembler/Disassembler). PAD збирає символи з кількох терміналів, формує з них пакети X.25 та спрямовує у мережу. Набір протоколів, що описують взаємодію не X.25 терміналів, зображений на рис. 27.5. До складу набору протоколів (**Triple X**) належать такі:

- X.3 – задає параметри PAD для асинхронного dte; дає змогу налагоджувати PAD для різних типів терміналів;
- X.28 – набір команд між асинхронним dte та портом X.3 модуля PAD; процедури приєднання dte до PAD; контроль з боку dte за функціонуванням PAD;
- X.29 – протокол обміну між X.25 dte та PAD або між двома PAD; зміна параметрів PAD з боку мережі в інтерфейсі PAD–мережа та PAD–віддалене dte.

Додаткові стандарти. Крім названих стандартів, у мережах X.25 також використовують стандарти X.32 та X.75.

Стандарт X.32 або Dial X.25 дає змогу користувачам одержати доступ до мереж X.25 через стандартні аналогові комутовані телефонні лінії, а не через призначені синхронні лінії, як у випадку X.25. Стандарт X.75 дає змогу сполучати різні мережі X.25 в одну.

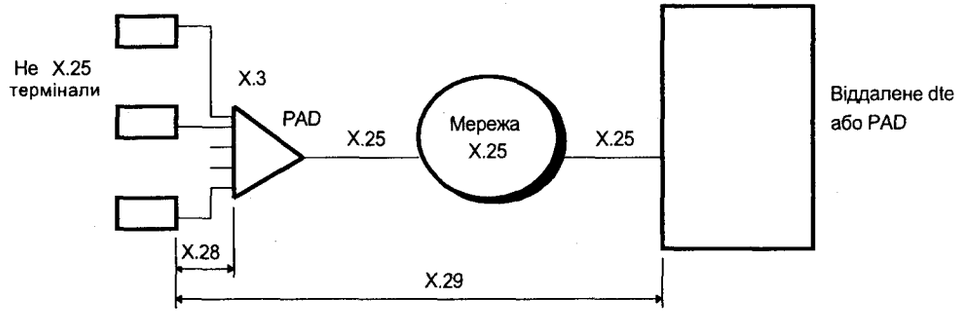


Рис. 27.5. Протоколи взаємодії терміналів.

Підсумки. Отже, переваги мережі такі:

• надійність – правильність передавання перевіряється у кожній ланці передавання; якщо виникає збій у мережі, то автоматично відбувається перемаршрутизація;

• гнучкість – можливі сполучення ЛМ–ЛМ, гост–гост, термінал–гост;

• сумісність; загальноприйнятий стандарт ITU; підтримує велика кількість виробників обладнання;

• захист; дає змогу створювати замкнені групи користувачів та керувати правами доступу членів цих груп.

До недоліків мережі X.25 належать такі:

• обмежений діапазон швидкостей. X.25 – це низькошвидкісна WAN-технологія, що оперує зі швидкостями від 2.4 до 64 Кбіт/с. Це не дає змоги передавати мультимедійну інформацію;

• низька перепускна здатність. X.25 – це комплексний протокол з потужними засобами захисту від спотворень передавання та збоїв. Велика питома вага операцій перевірки коректності та частота їх виконання призводять до різкого зменшення перепускної здатності (пакет затримує та перевіряє кожен вузол).

27.2. Мережа Frame Relay

Технологія ретрансляції кадрів **Frame Relay (FR)** виникла завдяки потребі сполучення локальних мереж каналами глобальних мереж, поєднання територіально розрізнених локальних мереж корпорації в єдину швидкісну корпоративну мережу. Frame Relay можна розглядати і як спрощений варіант X.25 для надійних мереж та високих швидкостей передавання даних. Головна відмінність цієї мережі від X.25 – це те, що корекцію помилок виконують не проміжні, а кінцеві вузли. Вузол мережі Frame Relay виконує такі дві головні функції:

• перевіряє цілісність кадру; якщо кадр спотворений, його відкидають;

• перевіряє правильність адреси; якщо адреса не відома, кадр відкидають.

Завдяки зменшенню часу на опрацювання у проміжних вузлах затримка у вузлі FR становить близько 3 мс, тоді як аналогічне значення для X.25 – 50 мс. Швидкість передавання FR набуває різних значень – від 56 Кб/с до 1.544 Мб/с залежно від перепускної здатності та кількості задіяних каналів. Технологія FR не накладає обмежень на максимальну швидкість передавання.

Аналогічно до X.25, технологія FR визначає тільки інтерфейс **UNI** (User to Network Interface) між DTE та DCE, не обмежуючи протоколів та архітектури магістральної мережі (вона може, наприклад, бути мережею ATM або ISDN). Для сполучення двох мереж FR визначено інтерфейс **NNI** (Network to Network Interface).

Протокольні рівні Frame Relay. На відміну від X.25, FR оперує тільки двома рівнями протоколів (див. рис. 27.3). Фізичний рівень подібний до однойменного рівня технології X.25 та відображає аспекти приєднання DTE та DCE. До DTE приєднують різні мости, маршрутизатори, комутатори та пристрої, аналогічні функціонально до PAD (FPAD). Для керування передаванням даних використовують протокол **LAPD** (Link Access Protocol D – протокол доступу до каналу D). Це підмножина протоколу мережі ISDN (див. розділ 28). Кадр, що передається LAPD, відповідає стандарту ITU Q.922. Базова версія FR не реалізує багатьох функцій канального та мережевого рівнів (виявлення та корекція помилок, керування потоком), однак підтримує такі функції мережевого рівня, як маршрутизація та керування логічними каналами.

Передавання даних мережею Frame Relay. FR допускає змінну довжину кадру – від кількох байтів до 2000 байт. Гнучка зміна довжини кадру дає змогу налаштовуватися до зміни навантаження. З іншого боку, вона призводить до змінної затримки у передаванні інформації та неможливості роботи з ізохронними потоками (відео та аудіоінформація).

На відміну від X.25, FR використовує, головним чином сталі віртуальні канали **PVC** (Permanent Virtual Channel). У випадку розірвання зв'язку FR автоматично перемаршрутизовує сполучення. PVC автоматично виділяються під час приєднання до мережі. Перед початком сполучення користувачу забезпечують гарантовану швидкість передавання інформації (Commited Information Rate (CIR)). CIR можна розуміти як дозволену середню швидкість передавання інформації. Крім CIR, визначена максимальна швидкість передавання (Maximum Information Rate (MIR)). Кадри, одержані в діапазоні швидкостей до CIR, будуть передані, у діапазоні від CIR до MIR – можуть бути передані, а у діапазоні понад MIR – будуть відкинуті.

Альтернативою до використання PVC є застосування комутованих віртуальних каналів **SVC** (Switched Virtual Cirquit). На відміну від призначених, комутовані канали формуються (і переформовуються) під час передавання. Користувач PVC повинен перед початком передавання 'купити' певний PVC з визначеним CIR, він оплачує його незалежно від ступеня реального використання каналу. Користувач SVC оплачує реальні параметри трафіка. На початку передавання структура каналу PVC відома. Рішення про конфігурацію каналу PVC приймає адміністратор, а рішення про структуру каналу SVC – інтелектуальні вузли-комутатори.

Структура кадру та керування потоком. Структура кадру Frame Relay показана на рис. 27.6.

Рис. 27.6. Структура FR-кадру.

Кадри починаються комбінацією 01111110. Для коректного визначення прапорців використовують бітстафінг. Заголовок містить адресну та інформацію керування. Його структура зображена на рис. 27.7.

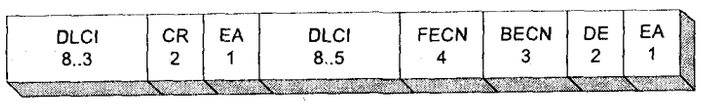


Рис. 27.7. Структура заголовка FR-кадру.

Коли в мережі Frame Relay нічого не передається, канал заповнюється комбінацією 'прапорець'. Отже, передавання у Frame Relay синхронне.

Десять біт адреси логічного каналу *DLCI (Data Link Connection Identifier)* – це головна адресна інформація. Стандарти ITU-T та ANSI допускають розширення адреси до 4 байт. У цьому випадку біт розширення адреси *EA (Extended Adress)* дорівнює одиниці.

Біт *CR (Command/Responce)* використовують протоколи верхніх рівнів. Біт розширення адреси *EA* є в кінці кожного байта. Якщо цей байт останній у заголовку, то біт дорівнює 1. Біти повідомлення про перевантаження *FECN (Forward Explicit Congestion Notification)* та *BECN (Backward Explicit Congestion Notification)* призначені для повідомлення наступного та попереднього у напрямі передавання даних вузлів про перевантаження.

Важливе значення для керування потоком має біт можливості знищення *DE (Discard Eligibility)*. Якщо цей біт у кадрі становить 1, то у випадку перевантаження мережі кадр знищується найперше. Задати біт *DE* може як користувач, так і апаратура передавання даних. У випадку перевантаження знищуються не тільки пакети з *DE*=1, якщо знищення цих пакетів не призводить до виправлення ситуації. Деякі провайдери Frame Relay дають суттєві знижки ціни, якщо користувач передає всі пакети з *DE*=1.

Інформаційне поле займає від одного до 1600 байтів. Перевіряльна послідовність займає два байти та формується з використанням циклічного коду.

Підсумки. Переваги FR-технології такі:

- висока перепускна здатність;
- одержання перепускної здатності на вимогу;
- сумісність з мережами ISDN, можливість використання інших мереж для транспортування.

До недоліків цієї технології належать такі:

- потреба у високоякісних каналах зв'язку;
- через відсутність механізму корекції помилок у проміжних ланках помилки виявляють тільки в абонента-адресата; це призводить до потреби повторення передавання всім маршрутом;
- непридатність для передавання ізохронної інформації;
- відсутність механізму простежування конфліктів у мережі.

Бібліографія та джерела

1. *Баранец С.* Введение в сети с коммутацией пакетов // Компьютерное обозрение. 1996. № 16(40).
2. *Крейнес А.* Пакет с нарочным // LAN Magazine. 1997. № 2.
3. *Парсонс Т, Бар Д.* Как стать победителем в гонке Frame Relay // LAN Magazine. 1996. № 5.

МЕРЕЖІ ISDN. ТЕХНОЛОГІЯ xDSL

Розділ 28

Мережа ISDN. Загальна характеристика та історія розвитку. Інтерфейси ISDN. Перехід до технології ISDN. Технологія xSDL: загальна характеристика, різновиди.

28.1. Мережі ISDN

Загальна характеристика та історія розвитку. Мережі **ISDN** (Integrated Services Digital Network – цифрові мережі інтегрованих послуг) з'явилися ще в 70-х роках XX ст. Власники провідних телефонних компаній світу дійшли висновку, що подальший розвиток аналогової телефонії безперспективний. Крім того, виникають потреби передати дані з високою швидкістю та надійністю. З цією метою була розроблена концепція цифрової мережі, а в 1976 р. введена в експлуатацію перша ISDN-станція. Згодом інтерес до технології ISDN послабився, оскільки вона виявилася досить дорогою та складною в установленні. Лише окремі фірми випускали пристрої та пропонували послуги ISDN. Водночас відбувався поступовий перехід технологій телефонних мереж у напрямі цифрових технологій ISDN (див. Д.28.1).

Сьогодні ISDN – це телефонна мережа з цифровими станціями, що сполучені цифровими каналами. ISDN комутує цифрові потоки даних. Цифро-аналогове та аналого-цифрове перетворення відбувається вже безпосередньо в ISDN-терміналі користувача.

ISDN реалізує концепцію розподіленої телефонної станції. В аналогових станціях у випадку транзитного сполучення утворюється петля (рис. 28.1,а). У мережах ISDN відбувається переадресація і петля знімається (рис. 28.1,б), тому немає місцевих та віддалених номерів і можна ввести єдиний план номерів для всієї мережі. Сполучення в ISDN-мережі відбувається майже моментально (30 мс). Тому навіть у великих мережах затримка у налагодженні не перевищує 0.2 с. Обов'язковою функцією мереж ISDN є маршрутизація сполучень.

Інтерфейси мережі ISDN. У технології ISDN визначено такі інтерфейси:

- **BRI** (Basic Rate Interface – інтерфейс базової швидкості, базового доступу; інтерфейс користувача) – визначає сполучення між абонентом та ISDN-станцією;
- **PRI** (Primary Rate Interface – інтерфейс первинної швидкості, магістральний інтерфейс) – визначає сполучення між проміжними ISDN-станціями.

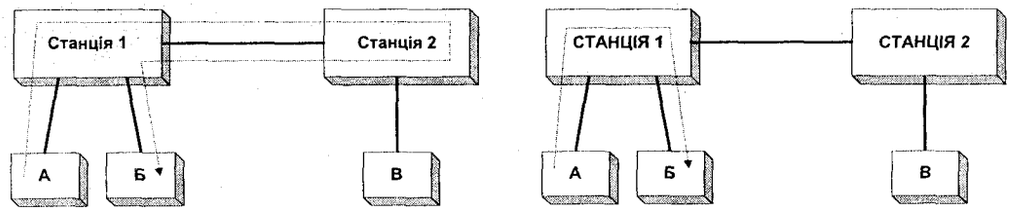
Інтерфейс базового доступу BRI визначено для скрученої пари. BRI – це структурований цифровий потік зі швидкістю 192 Кбіт/с, розділений на такі частини:

$$192=144+48,$$

де потік швидкості 48 Кбіт/с містить біти синхронізації та корекції помилок, а потік швидкості 144 Кбіт/с, відповідно, поділяється ще на три потоки:

• два (канали **B**) по 64 Кбіт/с, які переносять інформацію користувача;

• один (канал **D**) – 16 Кбіт/с, що використовується для керування. Канал D передає адресну інформацію, сигнали виклику та інші дані керування. Він може обслуговувати кілька каналів B. Враховуючи структуру каналів, кажуть, що *BRI=2B+D*.



а *б*

Рис. 28.1. Сполучення петлею (*а*) та його уникнення (*б*).

Залежно від фізичної реалізації BRI буває двох типів: **U** та **S/T**. Інтерфейс U призначений для роботи з віддаленим абонентом. Він використовує скручену пару, якою можна передавати дані на відстань 4–7 км. У U інтерфейсі реалізовано повнодуплексне передавання. Інтерфейс S/T розроблений для роботи всередині офісу чи квартири; відстань передавання – декілька сотень метрів по чотирипроводовому кабелю.

Магістральний інтерфейс PRI використовують для зв'язку телефонних станцій ISDN. У загальному випадку

$$PRI=nB+D.$$

У США та Японії, де застосовують цифрові канали T1 (1544 Кбіт/с), PRI=23B+D. У Європі, де цифрові канали E1 (2048 Кбіт/с), PRI=30B+D. Фізично PRI є звичайним для аналогової телефонії трактом з імпульсно-кодовою модуляцією. Однак логічно ІКМ та PRI несумісні.

28.2. Технологія xDSL

Технологію **DSL** (Digital Subscribers Line) розроблено одним із дослідницьких підрозділів компанії Bell Operating Company у 1987 р. Учені поставили собі за мету створити сучасну високошвидкісну технологію, яка б максимально використовувала наявні мідні мережі.

Пояснити технологію DSL можна, якщо порівняти передавання даних звичайним 'телефонним' модемом та модемом DSL. Відомо, що на сигнали, які передаються телефонною лінією, впливають сильні завади. Модеми призначені усунути цей вплив за допомогою спеціальних алгоритмів кодування, опрацьовуючи сигнал на сигнальних процесорах та адаптивно узгоджуючи параметри сигналу і лінії. DSL-прилади мають схеми кодування 2B1Q, CAP, DMT з невеликою шириною смуги перепускання та небагатьма кодовими станами. Ці методи

кодування дають змогу збільшити ступінь стиснення даних і в результаті збільшити швидкість їх передавання. Сигнальні процесори DSL-технології застосовують модель мідного дроту, що дає змогу врахувати вплив завад.

Схему кодування 2B1Q використовують також і в технології ISDN. Схема CAP розроблена фірмами Shmid Telecommunications та Lucent Technologies і відповідає стандарту G.821, схема DTM – фірмою Northern Telecom.

Сьогодні відомі декілька технологій DSL:

• **HDSL** (High bit rate DSL) використовує симетричні потоки в обох напрямах, швидкість 1.5–2.0 Мбіт/с;

• **ADSL** (Asymmetric DSL) використовує асиметричні потоки, один (від сервера до користувача) інтенсивніший; цю технологію застосовують в Internet (пор. з технологією DirecPC); швидкість передавання в одному потоці 1.5–6.0 Мбіт/с, в іншому 64–640 Кбіт/с;

• **RADSL** (Rate Adaptive DSL) адаптивна до швидкості, тобто в ній автоматично обирається оптимальна швидкість щодо якості каналу (пор. з налагоджуванням швидкості у модемах). Швидкості передавання є в інтервалах 600 Кбіт/с – 7 Мбіт/с для одної лінії та 128 Кбіт/с – 1 Мбіт/с для іншої;

• **SDSL** (Single line Symmetric DSL) використовує симетричні потоки в обох напрямах. Швидкість передавання всюди 384 Кбіт/с;

• **VDSL** (Very High bit rate DSL) має дуже високі швидкості передавання: для низхідного потоку – 51 Мбіт/с, а висхідного – від 1.6 до 2.3 Мбіт/с. Відстань передавання обмежена – 100–300 м.

На відміну від технології ISDN, технологія xDSL використовує призначені канали зв'язку і працює одночасно з традиційним телефонним обладнанням. Для передавання даних застосовують спеціальний xDSL-модем. Технологія xDSL не передбачає перебудови лінійного обладнання мережі, як ISDN.

Бібліографія та джерела

1. *Волобуев Д.В.* Второе пришествие ISDN // Сети. 1995. № 4.
2. *Иванов В., Чепусов Е, Шаронин С.* Вторая жизнь медного кабеля // LAN Magazine. 1997. № 2.
3. *Иносе Х.* Интегральные цифровые сети связи: введение в теорию и практику. М .: Радио и связь, 1982.

ДОДАТОК ДО РОЗДІЛУ 28

Д.28.1. Перехід до технологій ISDN

Розвиток телефонних мереж пройшов чотири стадії. Спочатку була звичайна аналогова мережа з аналоговими АТС та телефонними каналами (рис. Д.28.1,*а*). З часом, коли кількість ліній збільшилася, виникла потреба їх концентрувати (ущільнити). На магістральних сполученнях почали використовувати цифрові сполучення інтерфейсу **DTI** (Digital Trunk Interface) (рис. Д.28.1,*б*). Аналогом цих сполучень є канали ІКМ-30 (120, 480); число *30* визначає кількість каналів у тракті. Потім з'явилися окремі ISDN АТС, які передавали інформацію цифровими телефонними трактами, надавали користувачу повний обсяг послуг ISDN, працюючи як зі спеціалізованими ISDN-терміналами, так і зі звичайними аналоговими телефонними апаратами (рис. Д.28.1,*в*). Остання стадія переходу до мереж ISDN – заміна застарілих аналогових АТС станціями ISDN (рис. Д.28.1,*г*).

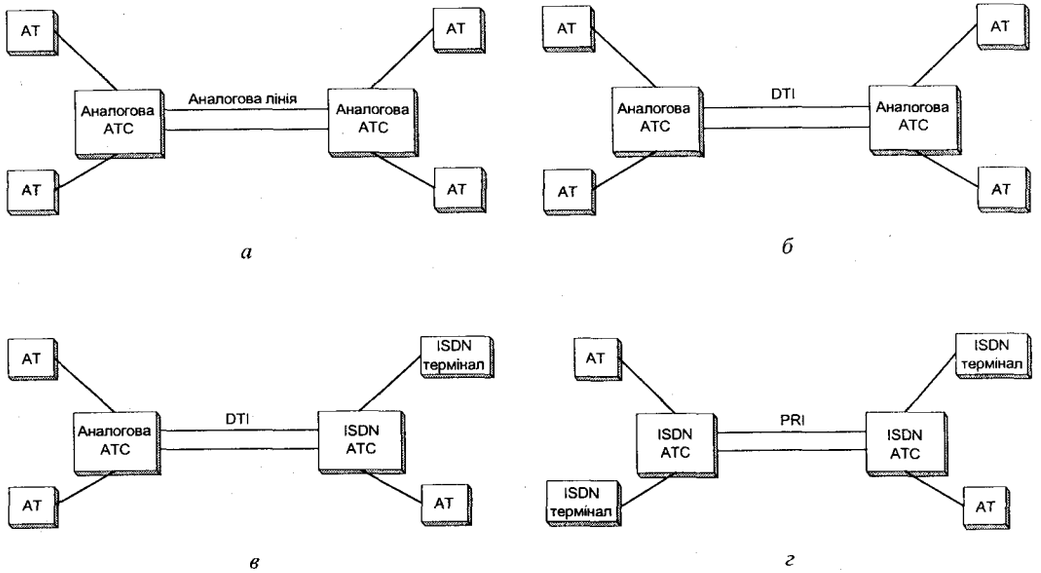


Рис. Д.28.1. Перехід до технологій ISDN.

ТЕХНОЛОГІЯ АТМ

Розділ 29

Загальна характеристика. Топологічна структура й головні елементи. Адресація та маршрутизація в мережі АТМ. Стандарти АТМ. Класифікація мереж АТМ. Етапи переходу до мереж АТМ. Взаємодія ЛМ та мереж АТМ. Технології LANE та MPOA.

29.1. Загальна характеристика

Мережі технології **АТМ** (Asynchronous Transfer Mode – режим асинхронного передавання) – це новітні пакетні мережі з інтеграцією послуг і великою швидкістю передавання інформації. Така технологія, як прогнозують учені, протягом 5–10 років замінить теперішні локальні та глобальні мережі. Головні властивості мереж технології АТМ такі:

• по-перше, це пакетна мережа з віртуальними каналами. Для передавання даних використовують пакет з фіксованим розміром 53 байти, який назвали *коміркою (cell)*. Це дає змогу апаратно реалізувати багато функцій опрацювання та маршрутизації, отже, різко зменшити тривалість опрацювання комірки, а також нормувати його. Стала тривалість затримки комірки має велике значення для ізохронного передавання аудіо- та відеоінформації;

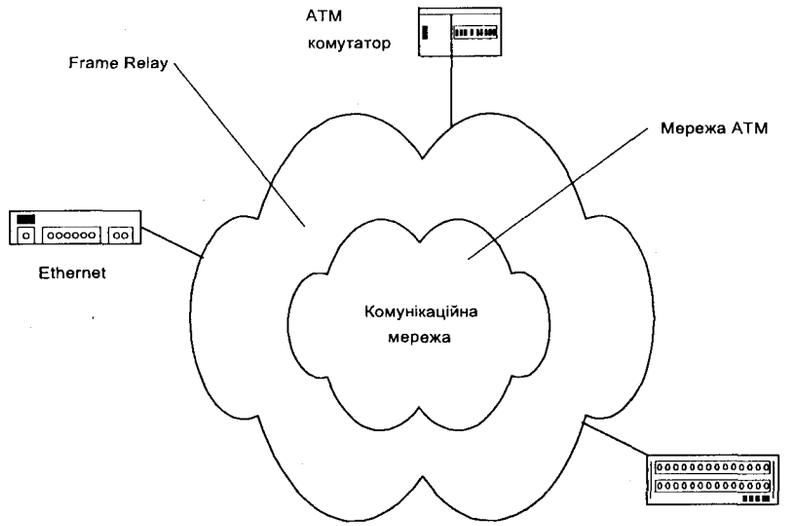


Рис. 29.1. Структура мережі АТМ.

• по-друге, це мережа інтегрованих послуг, тобто у ній єдиним потоком передається інформація з різними вимогами до затримок передавання та достовірності (аудіо-, відеоінформація, дані, інформація електронних систем сигналізації тощо). Для передавання відеоінформації, як звичайно, потрібна велика перепускна здатність, а для передавання телефонних розмов – мала. Під час передавання аудіо- або відеоінформації невелике спотворення даних цілком допустиме і суттєво не впливає на якість сигналу, а під час передавання даних спотворення навіть одного біта недопустиме. Водночас під час передавання аудіо- та відеоінформації потрібна стала швидкість передавання, а під час передавання даних швидкість може бути змінною;

• по-третє, швидкість та якість передавання інформації в мережі ATM задають за запитом користувача. Ця мережа працює як з вузькосмуговими (швидкість 9600 біт/с – 2 Мбіт/с), так і з широкосмуговими каналами (2–622 Мбіт/с і більше);

• по-четверте, мережа ATM описує тільки інтерфейсні характеристики і для передавання даних може використовувати широкий спектр реальних каналів та комунікаційних мереж (рис. 29.1). З іншого боку, для зовнішнього користувача вона може надавати сервіс багатьох мереж та протоколів (Frame Relay, X.25, TCP/IP, SPX/IPX та ін.);

• по-п'яте, ця мережа гнучка в експлуатації. Якщо трапляється збій або потрібно збільшити пропускну здатність, автоматично вибираються нові шляхи передавання з врахуванням вимог кожної комірки.

29.2. Топологічна структура та головні елементи мережі

Мережа ATM складається з комутаторів ATM, магістральних каналів зв'язку та робочих станцій з адаптерами ATM (рис. 29.2). Вона має зіркоподібну топологію.

Адаптери ATM розміщені безпосередньо на робочих станціях, мають потужний RISC процесор та виконують функції з опрацювання комірок відповідно до вимог стандарту UNI. Вартість адаптерів ATM сьогодні значно перевищує вартість мережевих адаптерів ЛМ.

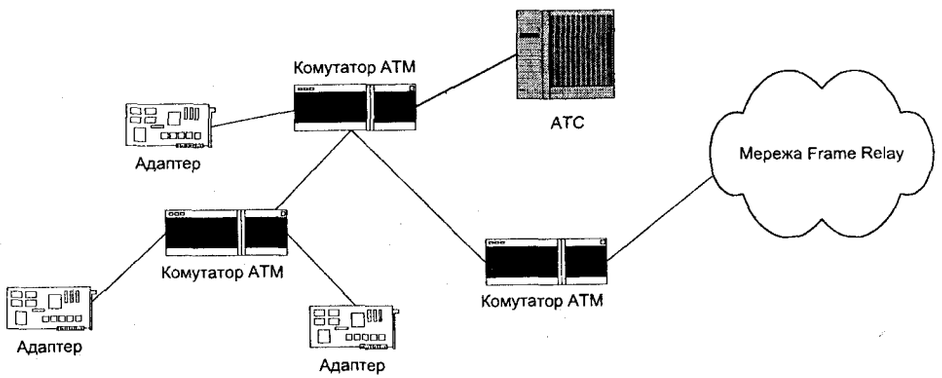


Рис. 29.2. Топологія мережі ATM.

Адаптер з комутатором ATM сполучений скрученою парою. Процедури зв'язку описує специфікація **UNI**.

Комутатор ATM виконує функції маршрутизації комірок, адресації, мультиплексування та демультиплексування потоків інформації. Це головний і найдорожчий елемент мережі ATM. Комутатори ATM за функціональними можливостями поділяють на такі:

• комутатори для невеликих робочих груп;

• комутатори для середніх та великих підприємств;

• граничні комутатори.

Магістральними для передавання даних між комутаторами ATM можуть бути канали T1, E1, T3, E3, SONET і навіть звичайні канали комутованої телефонної мережі. Найбільшу швидкість передавання даних сьогодні мають канали специфікації SDH (622 Мбіт/с). Передавання даних магістральними каналами між комутаторами регламентує специфікація **NNI**.

29.3. Адресація та маршрутизація в мережі ATM

У мережі ATM, подібно до Frame Relay, функцію корекції помилок виконують протоколи верхнього рівня у відправника та одержувача інформації. Комутація комірок відбувається незалежно від їхнього змісту. Структури комірок протоколів UNI та NNI незначно відрізняються (рис. 29.3). Кожен комутатор працює тільки з заголовком комірки. За інформацією з заголовка визначають адресу призначення комірки, її тип та пріоритет. Від типу комірки (дані, відеоінформація) залежить її пріоритет. Передавання відбувається з використанням віртуальних сполучень. Комірки передаються в чіткій послідовності номерів.

В ATM можна використовувати один з двох типів віртуальних сполучень:

• комутоване **SVC**;

• постійне **PVC**.

SVC створює тимчасові віртуальні сполучення, а PVC подібне до призначених ліній та формується на постійній основі.

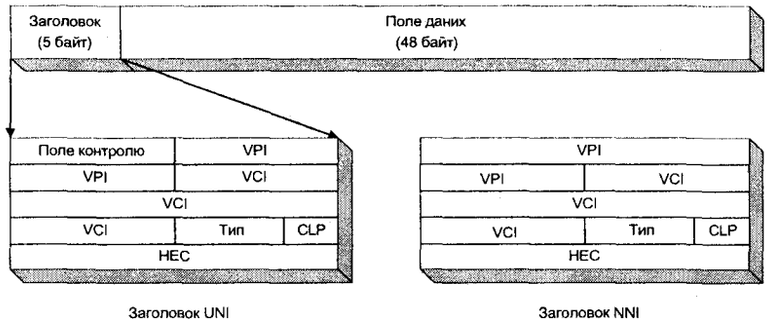


Рис. 29.3. ATM-структури.

Віртуальні сполучення ATM можуть працювати зі сталою швидкістю передавання **CBR** (Constant Bit Rate) – для передавання мовленнєвого або відеотрафіку, або зі змінною бітовою швидкістю **VBR** (Variable Bit Rate) для передавання даних. Кожне віртуальне сполучення має власний набір параметрів (**MCR** (Minimum Cell Rate), **SCR** (Sustained Cell Rate), **PCR** (Peak Cell Rate)), які визначають мінімальну, середню та максимальну допустимі швидкості передавання комірок.

Адреса в ATM-комірці має дві частини: ідентифікатор віртуального шляху **VPI** (Virtual Path Identifier) та ідентифікатор віртуального каналу **VCI** (Virtual Circuit Identifier). Шлях передавання комірки мережею складається з одного або більше віртуальних шляхів, які, відповідно, можуть мати кілька віртуальних каналів. VPI та VCI відповідають тільки конкретному сполученню на визначеному шляху передавання і мають локальне значення для кожного комутатора. Комутатор ATM транслює вхідні значення VPI та VCI у вихідні. Вибір віртуального каналу в межах шляху залежить від типу трафіку (дані, аудіо, відео) та його пріоритету.

29.4. Стандарти ATM

Стандарти ATM розробляють кілька організацій: ATM Forum, Frame Relay Forum, Internet Engeneering Task Force (IETF), ISO. ATM за міжнародними стандартами – це технологія передавання інформації широкосмугових цифрових мереж з інтеграцією служб (B-ISDN).

B-ISDN описує функції ATM за допомогою багаторівневої моделі, подібної до еталонної моделі взаємодії відкритих систем. Модель протоколу B-ISDN перевизначає три нижні рівні як фізичний, рівень ATM, рівень адаптації ATM. Нижні рівні, як звичайно, реалізуються апаратно, а верхні – програмно (рис. 29.4).

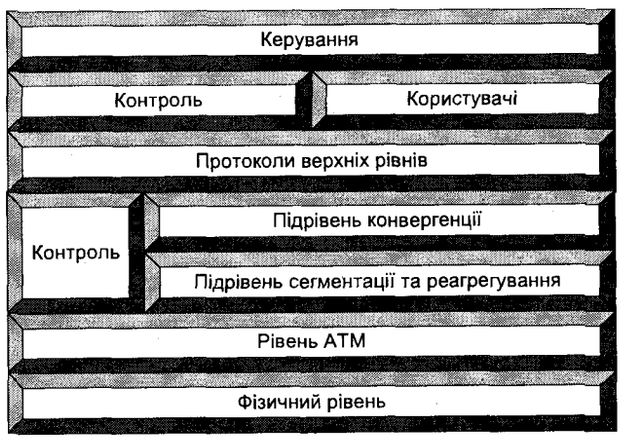


Рис. 29.4. Рівні опрацювання ATM-комірок.

Фізичний рівень визначає інтерфейс з середовищем передавання (фізичний інтерфейс, швидкості передавання та спосіб перетворення ATM-комірок у сигнал на лінії зв'язку). ATM не залежить від типу фізичного середовища. Передавання даних може відбуватися через різні інтерфейси: SDH, T1/E1, T3/E3, і навіть через модеми зі швидкістю 9.6 Кбіт/с. Головними факторами для вибору фізичного носія є швидкість та перепускна здатність.

На фізичному рівні визначено два підрівні:

- підрівень, який залежить від фізичного середовища (Physical Media Dependent (PMD));
- підрівень конвергенції трансмісії (Transmission Convergence (TC)).

PMD пов'язаний з такими характеристиками фізичного рівня, як тип фізичного сполучення, швидкість передавання в ньому. Підрівень TC реалізує одержання інформації з фізичного рівня. На ньому відбуваються генерація та перевіряння кодів корекції помилок у заголовку (Header Error Correction (HEC)), виділення комірок з потоку бітів та опрацювання порожніх комірок.

Рівень ATM працює з ATM-комірками (див. рис. 29.3). Кожна комірка складається з заголовка (5 байт) та поля даних (48 байт). Розмір поля даних – компроміс між короткими та довгими комірками. Довгі комірки ефективні під час передавання даних. У них питома вага інформації керування зменшується. Однак для довгих комірок тривалість передавання нерівномірна. Короткі ж комірки забезпечують рівномірніший розподіл часу й ефективні для передавання аудіо та відеоінформації.

Рівень адаптації ATM. Головне призначення рівня адаптації ATM (ATM Adaptation Layer (AAL)) – це об'єднання даних від джерел з різними характеристиками та типами інформаційних потоків. Рівень AAL приймає дані від протоколів верхнього рівня і перетворює їх у 48-байтові сегменти, які розміщуються в полі даних комірки. Залежно від типу даних AAL визначає параметри класу сервісу. Є такі класисервісу:

- A (1, AAL1) – орієнтований на сполучення зі сталою бітовою швидкістю для ізохронного передавання синхронної інформації;
- B (2, AAL2) – орієнтований на сполучення зі змінною швидкістю для передавання синхронних даних (наприклад, для передавання стиснутої аудіо- та відеоінформації);
- C (3, AAL3) – орієнтований на сполучення зі сталою швидкістю в асинхронному режимі роботи для передавання інформації локальних мереж;
- D – не орієнтований на сполучення, підтримує асинхронний режим роботи;
- X – з налагодженням сполучення, для якого адміністратор визначає параметри трафіку та якість обслуговування;
- Y – з максимальною якістю (best-effort), яку можна досягти в конкретних умовах;
- AAL5 – орієнтований на сполучення зі змінною швидкістю передавання. Не потребує синхронізації (наприклад, для передавання даних X.25 або Frame Relay).

Рівень адаптації ATM складається з двох підрівнів:

- конвергенції (Convergence Sublayer(CS)) – визначає потрібний клас обслуговування та параметри передавання;
- сегментації і реагрегування (Segmentation and Reassembly Sublayer (SAR)) – збирає та розбирає комірки.

29.5. Класифікація мереж ATM

Сьогодні можна виділити такі три галузі використання ATM з різними вимогами:
- локальні мережі ATM-LAN;
- територіальні, глобальні мережі ATM-WAN;
- мережі ATM для центральних офісів ATM-CO.

Локальні мережі ATM посідають найнижчу сходинку в ієрархії ATM-систем. Їхня перепускна здатність становить 1–2 Гбіт/с. Головні вимоги – висока перепускна здатність та можливість приєднання максимальної кількості станцій. Високої перепускної здатності можна досягти за допомогою волоконно-оптичних кабелів.

Обладнання для мереж ATM-LAN – це ATM-комутатори, маршрутизатори, блоки приєднання, мости та робочі станції. ATM-комутатор забезпечує великій кількості користувачів швидкий доступ до мережевих ресурсів (наприклад, сервера та маршрутизатора). Маршрутизатори ATM підтримують численні протоколи маршрутизації та перетворюють їхні пакети в пакети для передавання через глобальні мережі ATM-WAN.

До локального ATM-комутатора можна приєднати робочі станції, сервери та концентратори. Таким чином формують інфраструктуру для робочої групи з високою продуктивністю.

Сьогодні, незважаючи на те, що вартість адаптерів ATM зменшується, вони недоступні для більшості користувачів.

Територіальні, глобальні мережі ATM об'єднують загальнодоступні та корпоративні глобальні мережі. Для їхнього функціонування потрібно орендувати канали зв'язку з досить високою вартістю. *Однак головна проблема – забезпечити ефективне використання засобів* зв'язку. Перепускна здатність таких систем – від 5 до 20 Гбіт/с.

Мережі ATM для центральних офісів – це надвеликі системи, які підтримують найбільшу кількість користувачів та служб (ATM-CO). Перепускна здатність мереж ATM-CO є в межах 20–100 Гбіт/с. Сьогодні виробники ATM-комутаторів постачають тільки 'базові' версії пристроїв, які ще не забезпечують побудови достатньо потужних систем. Системи ATM-CO, як і ATM-LAN, використовують волоконно-оптичні лінії зв'язку. Головними вимогами до таких систем є здатність до керування та нарощення, яка б гарантувала тривалий термін служби.

29.6. Етапи переходу до мереж ATM

Зважаючи на наявність великої кількості локальних та глобальних мережевих систем, несумісних з технологією ATM, великі фірми-розробники програмного забезпечення передбачають поступовий перехід до мереж ATM. Зокрема, фірма Novell пропонує такі стадії переходу.

1. Сполучення ЛМ. Мережа ATM розташована між маршрутизаторами та замінює канали T1, служби ретрансляції кадрів. Інкапсульований трафік ATM переноситься через середовище ATM. Сегменти зв'язані через маршрутизатори.

2. Емуляція ЛМ. Робочі станції сприймають мережу ATM як Ethernet або Token Ring. Кадри ЛМ розділені на менші частини та інкапсулюються в комірках ATM. Вони спрямовуються у вибрані пункти призначення з заданими швидкостями. У цьому випадку користувач не має географічних обмежень. Зникає різниця між глобальними та локальними мережами. Для реалізації цього етапу потрібно розробити драйвери ATM з інтерфейсом ODI. Однак для таких систем також необхідно використовувати маршрутизатори, які проте звужують смугу перепускання та викликають непередбачені затримки.

3. Чиста ATM. Фірма Novell розробляє версію протоколу IPX, орієнтовану на налагодження сполучення і сумісну з ATM (гарантована смуга перепускання та малі затримки), а також інфраструктуру, яка підтримуватиме логічний рівень об'єднання мереж і буде моделлю фізичної мережі. Ця логічна можель дасть змогу мережі ATM та мережевим середовищам, таким як Ethernet, Token Ring, FDDI, Arcnet, виглядати єдиною мережею.

29.7. Взаємодія локальних мереж та мереж ATM

Незважаючи на те, що технологія ATM підтримує передавання даних як у локальних, так і в глобальних мережах, у сфері локальних мереж вона не стала популярною. Деякі фахівці вважають, що ATM на 25 Мбіт мертва. Класичні технологічні вирішення для локальних мереж (особливо з появою Fast та Gigabit Ethernet'у) значно дешевші, ліпше інтегруються з наявними структурами, простіші в обслуговуванні, ніж відповідні вирішення ATM.

Водночас технологію ATM впроваджують для швидкісних магістралей та для передавання даних на великі відстані. Постає завдання організувати передавання даних зі звичайних локальних мереж у мережу ATM або між двома локальними мережами, що сполучені магістраллю ATM. Для вирішення цього завдання розроблено та стандартизовано низку підходів.

Classical IP over ATM. Стандарт розроблено IETF. Це найпростіше вирішення, яке дає змогу передавати пакети та перетворювати IP-адреси в ATM- і навпаки. Станції (маршрутизатори, комутатори, інші пристрої, що мають IP-адресу) приєднані до мережі ATM. Кожній станції відомі її IP- та ATM-адреси, які вона повідомляє серверу ATMARP. Для сполучення двох станцій можна використовувати як постійний (PVC), так і комутований віртуальний канали. У першому випадку адміністратор вручну формує маршрутні таблиці, в яких кожній IP-адресі одержувача відповідають ATM-адреси, які використовують для налагодження віртуального каналу. Якщо потрібно використати SVC, ATM-адресу станції призначення дізнаються на сервері ATMARP. Після налагодження каналу станції самостійно передають дані, перетворюючи IP-пакети в ATM-комірки та навпаки.

Таке вирішення має низку обмежень. Найсуттєвішим є те, що робочі станції та сервер ATMARP повинні бути в одній логічній (віртуальній) локальній мережі. Якщо потрібно сполучити станції у різних локальних мережах, то кожна з них налагоджує віртуальний канал з маршрутизатором. У цьому випадку маршрутизатор може суттєво знизити швидкість передавання. Іншим недоліком є обмеження типів пакетів тільки IP-пакетами – не підтримується багатопротокольне передавання, не можна також використати можливості мереж ATM щодо задання якості сервісу.

LAN Emulation (LANE). Стандарт розроблено ATM Forum. Він дає змогу сполучати дві локальні мережі магістраллю ATM. Як і в попередньому випадку, станції, що сполучаються, належать до однієї віртуальної мережі (проте можуть належати до різних фізичних мереж).

LANE емулює MAC-підрівень протоколу канального рівня. Тому передавання для протоколів мережевого рівня прозоре. Послугами LANE можуть користуватися довільний протокол мережевого рівня і декілька протоколів одночасно.

Стандарт LANE визначає два інтерфейси: між робочою станцією (або іншим пристроєм, на якому розміщено клієнта LANE) і мережею **LUNI** (LANE User to Network Interface) та між мережами **LNNI** (LANE Network to Network Interface).

Історично першим було розроблено LUNI (LANE 1.0). Цей інтерфейс описує передавання даних між кінцевими станціями, які є в одній локальній мережі. Він передбачає взаємодію клієнтів LANE та служб LANE. Розрізняють три такі служби:

- сервер LANE – перетворює MAC-адреси в ATM-адреси;
- сервер конфігурації LANE – повідомляє клієнтам LANE ATM-адреси служб LANE;
- сервер циркулярних передавань LANE (LANE Broadcast/Unknown Server – LANE BUS).

Фізично ці сервери можуть бути в одному пристрої. Для сполучення клієнтів LANE та служб сьогодні, як звичайно, використовують комутовані віртуальні канали (SVC).

Передавання з використанням LANE відбувається так. Припустимо, що користувач станції хоче передати інформацію на станцію в іншій локальній мережі. Спочатку клієнт LANE цієї станції визначає, чи знає він ATM-адресу сервера LANE. Якщо ця адреса невідома, то станція звертається за довідкою до сервера конфігурації LANE. Якщо ж і сервер LANE не знає адреси станції-одержувача, то він звертається до сервера LANE BUS. Цей сервер шляхом циркулярних передавань запитує ATM-адреси всіх станцій локальної мережі й після одержання інформації передає її серверу LANE.

Знаючи ATM-адресу станції-одержувача, клієнт налагоджує з нею віртуальний канал та організовує передавання, формує і передає ATM-комірки, приймає комірки та збирає з них MAC-кадри (наприклад, Ethernet-кадри).

LUNI передбачає й емулювання дейтаграмних передавань. У цьому випадку клієнт передає комірки LANE BUS, який потім ретранслює їх на станцію призначення.

Стандарт LANE 1.0 не описував інтерфейсу LNNI і в такій мережі міг бути тільки один сервер LANE. У великих мережах цей сервер ставав вузьким місцем та обмежував продуктивність. Стандарт LANE 2.0 впроваджує стандарт LNNI та передбачає взаємодію кількох серверів LANE (до 20 серверів LANE та LANE BUS). Компоненти служб LANE розподілені по мережі.

Стандарт LANE має свої обмеження. Як і технологія Classical IP over ATM, він діє в межах однієї логічної локальної мережі. Для передавання між кількома локальними мережами треба використовувати маршрутизатор, який стає знову ж таки вузьким місцем системи. Технологія обмежена і за розмірами. Чим більше станцій, тим гірше працює мережа. Максимальна кількість станцій локальної мережі – 2000. LANE, як технологія канального рівня, не підтримує керування якістю сервісу, реалізованого на верхніх рівнях. Стандарт LANE 2.0 передбачає, щоб усі канали в емульованій мережі використовували один і той же тип швидкості трафіку (CBR – стала, VBR – змінна, UBR – невизначена, ABR – доступна бітова швидкість).

Multiprotocol over ATM (MPOA). Описані вище технології діють у межах єдиної віртуальної локальної мережі, а якщо потрібно сполучитися з іншою мережею, то вузьким місцем є маршрутизатор. Вирішити цю проблему дає змогу стандарт MPOA, розроблений ATM Forum. Стандарт MPOA взаємодіє з пристроями LANE і утворює з ними єдину систему. За його допомогою можна передавати інформацію між віртуальними локальними мережами без використання традиційних маршрутизаторів.

Стандарт MPOA передбачає наявність таких двох типів пристроїв:

- серверів маршрутизації (Route servers), які зберігають маршрутні таблиці, будують оптимальні маршрути, взаємодіють з іншими серверами та маршрутизаторами;
- кінцевих пристроїв (Edge devices) – клієнтів MPOA. Головна їхня функція – передавання та приймання даних.

Зазначимо, що головні компоненти MPOA – логічні. Їх можна реалізувати у вигляді окремих пристроїв, однак найчастіше вони працюють у складі інших пристроїв – гостів, комутаторів, адаптерних плат тощо.

Принцип роботи MPOA доволі простий. Обладнання локальних мереж приєднують до клієнтів MPOA, кожен з яких, відповідно, має безпосередній вихід у мережу ATM. Нехай робоча станція хоче налагодити сполучення з іншою станцією в іншій мережі. Вона передає найближчому клієнту MPOA пакет з адресами одержувача. Клієнт перевіряє MAC- або IP-адресу одержувача та шукає у своїх таблицях відповідну ATM-адресу. Якщо такої адреси немає, то він звертається до найближчого сервера маршрутизації. Сервер шукає адресу в своїх маршрутних таблицях. Якщо адресу відшукано, то її передають клієнту. Якщо ж потрібної адреси немає, то сервер звертається до інших серверів маршрутизації, використовуючи один з протоколів маршрутизації (наприклад, RIP, OSPF, NHRP, IPNNI).

Після визначення ATM-адреси призначення клієнт MPOA налагоджує з адресатом віртуальний канал і подальше передавання відбувається по цьому каналу поза сервером маршрутизації. Таке передавання називається *одноланковим* (one-hop routing). Таке сполучення вилучає сервер маршрутизації (маршрутизатор) як вузьке місце мережі.

У деяких випадках, особливо під час коротких передавань, коли час налагодження каналу сумірний з часом власне передавання, вигідніше організувати передавання без попереднього налагодження сполучення. Таке передавання називається *покроковою маршрутизацією* (hop-by-hop routing). У цьому випадку кінцеві пристрої спрямовують свої комірки до сервера маршрутизації, який ретранслює їх далі за обраним маршрутом (як це відбувається у традиційних маршрутизаторах). Відомі також і адаптивні вирішення, коли клієнт MPOA здатний визначати довгі та короткі передавання та перемикатися з одноланкової на покрокову схему передавання і навпаки.

Бібліографія та джерела

1. *Владимиров В.А.* Технология ATM: основные положения // Сети. 1996. № 2.
2. *Ковалерчик И.* ATM в реальном мире // Сети. 1997. № 7.
3. *Кроус Т.* Novell прокладывает дорогу к ATM // Сети. 1995. № 1.
4. *Петроски М.* Все ли готово для поддержки ATM // Сети. 1995. № 2.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ДІЯЛЬНОСТІ ГРУП

Передумови виникнення та історичний розвиток засобів організації роботи груп. Головні функції систем groupware. Огляд та порівняння наявних продуктів.

30.1. Передумови виникнення та історичний розвиток засобів організації роботи груп

Згідно з дослідженнями International Data Corporation (IDC), кінець 90-х років став визначальним у розвитку технології підтримки діяльності робочих груп. Сьогодні таку технологію використовують понад 30 мільйонів користувачів. У чому ж секрет такого бурхливого розвитку цих технологій?

Одночасно з появою та розповсюдженням комп'ютерної техніки та комп'ютерних мереж виникла потреба ефективніше організувати діяльність груп людей, що працюють над спільними проектами, мають спільні інтереси тощо. Історично першими виникли такі форми роботи груп, як *електронні дошки оголошень (Bulletin Board System (BBS))*, *електронна пошта*, *конференції*, пристосовані до невеликої швидкості роботи глобальних мереж. Тоді ж у локальних мережах виникла технологія конференції у реальному часі (chat-технологія).

Сьогодні активно розвиваються технології роботи груп. Наприклад, з'явилися технології відеоконференцій, web-технології, технології підтримки роботи організацій, автоматизації документообігу. Визначилася тенденція до інтеграції таких технологій у межах єдиного середовища роботи офісу, що дасть змогу автоматизувати роботу офісу, перейти до безпаперових технологій, проконтролювати порядок та стан виконання будь-якої роботи.

Технологія *електронних дощок оголошень* полягає в тому, що користувачі звертаються до центрального сервера. Через визначену інтерфейсну систему (найчастіше меню) вони можуть скопіювати файли з сервера на свою машину, а також передати свої файли. Отже, BBS працює як репозитарій інформації.

Технологія *електронної пошти* дає змогу абонентам, як уже зазначено, пересилати листи та файли. Для цього треба знати адресу абонента. Повідомлення електронної пошти, що надійшло, зберігається на локальному поштовому сервері, навіть якщо користувач відсутній, і надходить до користувача у випадку його ввімкнення в систему. Для роботи з поштою користувач має спеціальну програму і може виконувати над повідомленнями різні операції. Для зручності аналізу поштових надходжень кожне повідомлення, крім тексту, має тему (subject).

У технології *конференцій* користувачі, об'єднані спільними інтересами, організовують конференцію – постійний розділ на сервері, присвячений певній темі. У межах конференції

користувачі висловлюють свої думки та ознайомлюються з думками інших. Кожна конференція має адміністратора – людину, яка стежить за коректністю її проведення і дотриманням її тематики.

У конференціях реального часу територіально віддалені користувачі письмово висловлюють свої думки з певного приводу й одночасно бачать позицію інших учасників конференції. Сьогодні цю форму конференції доповнено безпосереднім аудіо та відеозв'язком.

Новий етап в історії систем підтримки діяльності груп розпочався 1986 р., коли фірма Lotus International випустила перший програмний продукт підтримки роботи груп. У той же час виник і спеціальний термін для позначення таких продуктів – **groupware**. Спеціалізовані продукти groupware фірм Lotus, Novell підтримують діяльність багатьох компаній. Ними користуються десятки мільйонів працівників. Водночас таке ПЗ досить дороге (до 1000–2000$ на одного користувача), його впровадження потребує грунтовного навчання персоналу, однак у користуванні воно не завжди просте.

Сьогодні системи groupware удосконалені завдяки появі та бурхливому розвитку intranet і web-технологій. Клієнт web-системи (браузер) простий у користуванні і є єдиним клієнтом в intranet-системі. Він може виконувати і функції підтримки групової діяльності. Вартість такого клієнта мінімальна (у багатьох випадках він взагалі безкоштовний). Термін для позначення таких систем – **intraware** (intranet+groupware).

30.2. Головні функції ПЗ підтримки робочих груп

З огляду на велику кількість різноманітних продуктів підтримки діяльності груп доцільно виділити головні функції таких продуктів, узагальнити їх, не прив'язуючи до продукту конкретного виробника. Такий підхід полегшує аналіз реальних продуктів.

Первинною функцією подібних систем є **електронна пошта**. На думку багатьох спеціалістів з розробки та впровадження інформаційних систем електронну пошту треба впроваджувати передусім, оскільки вона відразу дає відчутний ефект. Сьогодні засоби електронної пошти забезпечують обмін інформацією як у межах внутрішньокорпоративної системи, так і в зовнішній інформаційній мережі (Internet). Такою поштою передають, крім текстових повідомлень, також файли довільних форматів. Користувач має змогу організовувати свою кореспонденцію та аналізувати її, задавати спеціальні фільтри, які відбиратимуть або блокуватимуть надходження пошти від визначених користувачем авторів або на визначену тематику (можна використати шукання за заданими ключовими словами). Підтримуються також індивідуальні та колективні адресні книги. Списки розсилання повідомлень відповідають окремим групам одержувачів інформації.

Іншою важливою групою є **функції календарного планування**. Інформаційна система забезпечує ведення кожним користувачем комплексу щоденника, записника, особистого довідника. Крім індивідуальних, система може простежувати часові параметри розгортання спільних проектів і вести для них окремі щоденники, координуючи їх. Наприклад, вона відшукує вільний час усіх учасників групи для організації засідання з теми. Керівник групи може давати

учасникам групи конкретні доручення, простежуючи їх виконання в будь-який момент часу. Можна створювати мережеві графіки виконання проекту, аналізувати та оптимізувати їх.

Компонентою систем підтримки роботи груп є також **програмне забезпечення організації документообігу**. Воно дає змогу не тільки впорядкувати та оптимізувати документообіг організації, але й оперативно простежувати рух документів. Як звичайно, такі системи підтримують схеми руху конкретного типу документа з визначенням етапів, проміжних операцій (внесення проекту, погодження, візи, збирання довідок, призначення відповідальних та ін.). Рух документа відбувається в електронному варіанті, електронною поштою. Кінцевий варіант документа роздруковується. Інформаційна система дає змогу проаналізувати стан формування документа. Сформований та підписаний документ надходить в електронний архів і доступний для всіх уповноважених працівників у довільний час. Використання системи підтримки документообігу значно прискорює рух документів. Нерідко в інформаційній системі підтримки груп створюють спеціальні дискусійні бази даних з певних тем, проектів, що працюють в асинхронному режимі. Кожен учасник проекту працює зі змістом бази у зручний для нього час. У межах проекту часто створюють інформаційні репозитарії, у яких зберігають усю текстову, графічну та іншу інформацію щодо проекту.

Водночас система підтримки діяльності груп, як частина загальнокорпоративної інформаційної системи, повинна **мати доступ до** оперативних **даних** діяльності підприємства, що зберігаються, як звичайно, **в базах даних** однієї з **СКБД корпоративного класу** (Oracle, Informix, Sybase). Такі системи доцільно **інтегрувати з системами підтримки прийняття рішень**, сховищами даних (datawarehouse), з розвинутими функціями багатовимірного аналізу.

Отже, у системах організації групової роботи важливою є **система адміністрування**, яка поділяє користувачів на групи. Для неуповноважених осіб вона блокує доступ до конфіденційної інформації, автоматично простежує авторство зроблених правок та змін у документах, приховує факт наявності даних для окремих категорій користувачів та дає доступ іншим категоріям 'тільки для читання'. Водночас система адміністрування забезпечує максимальну продуктивність роботи адміністратора і мінімум помилок.

Сьогодні у зв'язку з бурхливим розвитком інформаційних web-технологій, побудовою мереж intranet принципи реалізації систем підтримки діяльності груп зазнають змін, щораз більше інтегруючись з корпоративними intranet-системами. Щораз частіше для доступу до даних використовують web-браузер. Головні тенденції цього етапу такі:

- **підтримка мобільних користувачів**. Користувач може увійти в корпоративну мережу з довільного комп'ютера, в довільній місцевості. Система повинна безпомилково ідентифікувати його, переслати його пошту, відновити зручне для цього користувача середовище роботи;
- **максимальна простота і зручність інтерфейсу**. Навіть дуже складна система повинна мати простий користувацький інтерфейс. Це робить користування зручним та збільшує коло користувачів і продуктивність їхньої праці;
- **інтеграція в застосування**. Як звичайно, найпоширеніші функції групової роботи інтегруються в застосування (такі як текстові процесори, електронні таблиці тощо);
- **автоматизація адміністрування**. Адміністративна система повинна швидко та ефективно адмініструвати великі мережі з сотнями серверів та тисячами і десятками тисяч клієнтів.

30.3. Огляд та порівняння наявних продуктів

Головними фірмами-виробниками програмного забезпечення підтримки діяльності груп є Lotus (власність IBM), Novell, Microsoft. Однак функціонально різні продукти подібні один до одного.

Компанія **Lotus**, яка є відомою на ринку засобів підтримки групової роботи такими класичними продуктами, як *Lotus Notes*, *Lotus Organizer* та іншими, випускає продукт Domino, що поєднує в собі Web-сервер та сервер Notes. Він дає змогу користувачам, що мають Web-браузери, працювати з базами даних Notes і мати доступ до всіх функцій цього пакета. Позитивною рисою Notes є простежування завдань та автоматизація ділових процесів. Оригінальною розробкою фірми є також Lotus Weblicator – модуль, що перетворює довільний браузер у реплікатор. Він дає змогу зберігати копії не тільки Web-вузлів, але й баз даних Notes, а тому локально заповнювати форми, а потім, якщо потрібно, пересилати їх на сервер.

Фірма **Microsoft** пропонує групове ПЗ *Exchange* з потужними функціями опрацювання повідомлень та автоматизації ділових процесів. Exchange Server 5.0 використовує захищений доступ до поштових скриньок, календарів та дискусійних форумів, дає змогу публікувати інформацію безпосередньо на Web-сервері. Універсальним клієнтом є програма *Outlook*. Фірма пропонує продукт браузер *Internet Explorer 4.0 Active Desctop* як майбутній універсальний інтерфейс доступу.

Для функціонування продукту *GroupWise 5* фірми **Novell** потрібен сервер Netware. За популярністю цей продукт майже зрівнявся з Notes (від 7 до 8 млн користувачів). Він має повний набір функцій підтримки діяльності груп. Доступ до всіх функцій відбувається через універсальну поштову скриньку (Universal Mailbox). Браузер GroupWise Web-Access дає змогу користувачам реєструватися на домашній сторінці GroupWise з довільного комп'ютера, приєднаного до Internet.

Крім великих фірм з потужними, багатофункціональними та дуже дорогими продуктами, на ринку засобів ПЗ для робочих груп є невеликі фірми з дешевими продуктами, що надають користувачу потрібний набір функціональних можливостей. Серед таких фірм великої популярності набула **Netscape** з продуктом *Communicator*, що складається з браузера Netscape, клієнта електронної пошти Messenger (підтримка інтерактивного змісту web-сторінок, фільтрування повідомлень, обмін цифровими візитками, шифрування, повідомлення з цифровими підписами), *Collabra* (дискусійні форуми, групи новин), *Composer* (редагування документів), *Conference* (електронна взаємодія у реальному часі, аудіоконференції, 'білі дошки', передавання файлів), *Calendar* (засіб групового планування), *AutoAdmin* (засіб блокування деякої інформації на настільних ПК так, що змінювати її можуть тільки адміністратори). Майбутня компонента *Constellation* збиратиме потрібну інформацію за запитом користувача та повідомлятиме його про це, *AppFoundry* – перший продукт у галузі автоматизації ділових процесів, є безкоштовним набором застосувань.

Серед продуктів невеликих фірм вирізняються *LiveLink Intranet* (**Open Text**) (керування документами, електронні конференції, організація групових проектів), *WebShare* (**Radnet**), *SamePage* (**WebFlow**).

30.4. Система підтримки діяльності груп GroupWise

Розглянемо головні архітектурні особливості та принципи побудови продукту Novell GroupWise.

GroupWise – це сервер-орієнтована система групової роботи. У ній реалізовані головні функції підтримки такої роботи. Система побудована як сукупність баз даних. Кожен користувач має БД поштових повідомлень, що містить персональну інформацію. До цієї бази можна приєднатися як через локальну мережу, так і через асинхронні канали чи X.25.

GroupWise має ієрархічну логічну структуру, яка складається з доменів, поштових відділень та об'єктів (рис. 30.1).

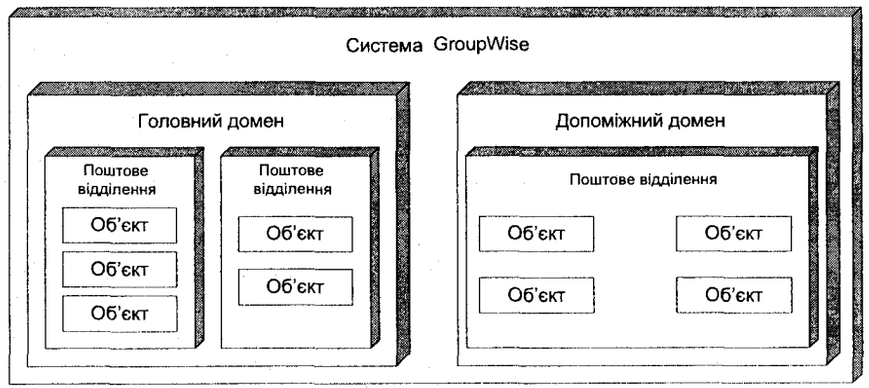


Рис. 30.1. Структура системи GroupWise.

Фізично домен та поштове відділення – це структури каталогів на одному чи кількох серверах. Система GroupWise добре масштабується – від одного домена та поштового відділення до багатьох доменів на багатьох серверах. Домен складається з поштових відділень та об'єктів і буває таких типів: головний, допоміжний, 'іноземний', зовнішній. Першим створюється основний домен, який керує і координує діяльність інших доменів. Він зберігає адресну інформацію, інформацію про конфігурування поштових відділень, об'єктів, тобто базу даних. Він підтримує синхронізацію БД доменів на різних серверах. Сервер повідомлень переносить повідомлення між поштовими відділеннями, доменами, системами.

Поштове відділення складається з поштових скриньок, кожна з яких – це персональна БД користувача. Користувачі однієї скриньки мають доступ до одного сервера. Користувачі одного поштового відділення можуть працювати в одному будинку, часто взаємодіють один з одним. Фізично поштова скринька – це набір баз даних та каталогів, у яких розміщена адресна інформація. На рівні поштового відділення діють два процеси: клієнтська програма (інтерфейс з електронною поштою, програмами планування, керування задачами, доступ до БД поштового відділення) та сервер поштового відділення. Клієнти підтримують платформи MS Win, DOS, Mac, Unix, Sun OS. Сервер поштового відділення керує передаванням файлів у межах цього відділення, у фоновому режимі виконує багато функцій клієнтської програми. Він взаємодіє з ПЗ адміністратора.

Кожен об'єкт має ідентифікатор, наприклад, domain.post office.object id. Найважливіші типи об'єктів такі:

- користувач;
- ресурс (конференц-зал, відеомагнітофон тощо);
- група (користувачі відділу тощо);
- псевдонім (наприклад, sysop).

Адміністративні функції системи: створення, конфігурування та інші операції з доменами, поштовими відділеннями, поштовими серверами та об'єктами.

Є програма адміністрування та сервер адміністрування. Окрема програма адміністрування конфігурує систему, працює з доменами, серверами повідомлень, виконує діагностичні перевірки, відображає структуру системи. Сервер адміністрування модифікує БД доменів та поштових відділень і виконує адміністративні функції, до яких програма адміністрування не має безпосереднього доступу (вони виконуються у фоновому режимі).

Головні функції системи такі:

універсальна поштова скринька. Всі повідомлення всіх типів збираються в єдиній поштовій скриньці, де їх класифікують, фільтрують;

електронна пошта;

персональний календар. Простеження персональних заходів. Різні типи їх відображення. Проектування власних відображень;

групове планування. Планування для користувачів, груп та ресурсів. Шукання вільного часу та виявлення конфліктів. Перевіряння індивідуальних календарів;

керування завданнями. Надання завдань співробітникам, стеження за виконанням та пріоритетами;

послідовна маршрутизація. Документ по черзі розсилається кожному адресату зі списку;

правила на сервері. Користувач заздалегідь визначає правила та дії, які виконуватимуться з повідомленнями: ретранслювання, делегування, знищення та ін. Правила спрацьовують, якщо виявлено задане слово або їхня комбінація;

контроль статусу. Простежування статусу повідомлення (де перебуває, стан, хто делегував та ін.). Повторне відсилання запитів;

повноваження. Задається список прав доступу, за яким користувач надає повноваження щодо доступу до окремих записів свого календаря. Можна створювати персональні недоступні повідомлення;

інформаційний сервер. Сервер публікує списки за темами. Абонентом такого списку може стати довільний користувач. Повідомлення пересилаються всім передплатникам;

Internet. Обмін електронною поштою через Internet та участь у диспутах. Повідомлення одержують через шлюз SMTP;

інтеграція з Netware. Сумісне адміністрування та синхронізація з NDS;

мобільні вирішення. Підтримка мобільних клієнтів.

Бібліографія та джерела

1. *Калман С.* Один ум хорошо, а два лучше // LAN. 1997. № 3.
2. *Карве А.* Открытый для дискуссий // LAN. 1997. № 3.
3. Увлеченные процессом // Сети. 1997. № 3.
4. *Шереметьев А.* Система групповой работы Groupwise v.4.1 // Компьютерпресс. 1997. № 2–4.
5. *Хиллз М.* Последнее слово в области группового программного обеспечения // Сети. 1997. № 3.

INTERNET TA WORLD WIDE WEB

Історія виникнення та еволюція Internet. Структура і принципи функціонування. Головні сервіси. Віддалений доступ. Передавання файлів. Електронна пошта. Телеконференції. Шукання інформації. Робота у World Wide Web.

У цьому розділі розглянемо розподілені інформаційні технології, які є у мережі Internet. Особливу увагу приділимо найважливішій технології – World Wide Web (WWW, Web-технологія, інколи її перекладають як ППП – Повсюдно Протягнуте Павутиння).

31.1. Історія виникнення та еволюція Internet

Мережа Internet розроблена Міністерством Оборони США як результат проекту ARPA (Advanced Research Projects Agency) у 1969 році. Тоді вона називалася ARPANET та об'єднувала університети й оборонні організації. У 1973 році ARPA розпочало дослідницький проект з об'єднання комп'ютерних мереж (Internetting project) за допомогою супутникових та радіоканалів. Головною проблемою було об'єднання різнотипних мереж. Тоді ж для вирішення цього завдання були винайдені шлюзи. Спочатку в ARPANET можна було тільки запускати програми на віддалених комп'ютерах, однак поступово до функціональних можливостей мережі додалися передавання файлів, електронна пошта, конференції та списки поштового розсилання. У 1983 р. було прийнято рішення використовувати на всіх вузлових машинах ARPANET протокольний стек TCP/IP, що визначило єдину платформу, ядро мережі. Тоді ж ARPANET розпалася на військову мережу MILNET і мережу університетів та інших наукових і державних установ ARPANET. Її використовували для досліджень з мережевої проблематики. У 1990 році ARPANET припинила своє існування. На базі технічної інфраструктури та розроблених принципів функціонування ARPANET виникла Internet. Організацією, яка активно зайнялася підтримкою розвитку Internet на цьому етапі, була NSF (National Scientific Foundation). Вона створила свою мережу NSFNET, яка об'єднала шість суперкомп'ютерів у логічне кільце каналами T3 (45 Мбіт/с) та була базовою в Internet. Сьогодні роль базових перейшла до мереж InternetMCI, Sprint Link, ANSNET.

31.2. Структура Internet

Internet – це '*інтермережа, що складається з багатьох мереж, які працюють на базі протоколів TCP/IP..., об'єднані шлюзами та використовують єдиний адресний простір і простір імен*'. Головною ознакою Internet є використання протоколів стека TCP/IP. Internet має

декілька опорних мереж, що надають магістральний, базовий сервіс. У США це InternetMCI, Commercial Internet Exchange, у Європі – EBONE, NORDUnet, DANTE, EUnet. Кожна з таких мереж відповідає за трафік всередині мережі та приєднання до інших мереж. Менші за розмірами регіональні та локальні мережі, які є частинами Internet, відповідають за передавання та одержання даних з Internet, зберігаючи повне адміністрування власними ресурсами та ведучи власну внутрішню політику. Отже, Internet – це конгломерат взаємоприєднаних та взаємодіючих мереж, у якому кожна з них зберігає повну внутрішню автономію та самофінансування.

31.2. Сервіси Internet

Найважливішими сервісами Internet є такі:
- емуляція термінала (віддалений доступ);
- передавання файлів;
- електронна пошта;
- телеконференції;
- WWW.

Командний інтерфейс більшої частини сервісів Internet ґрунтується на синтаксисі команд Unix.

Віддалений доступ (telnet). Telnet – це протокол віддаленого доступу, який дає змогу користувачу виконувати програми на інших машинах. Інтерфейс та набір команд telnet стандартизовано, а тому з довільного клієнта можна виконувати команди на довільному сервері. Структура команди telnet така:

```
% telnet адреса віддаленого комп'ютера.
```

Під час роботи з сервісом telnet є змога працювати з віддаленим комп'ютером та локальною машиною в командному режимі, до якого можна перейти за допомогою введення так званого Esc-символу (наприклад, ^]).

Власне з використанням telnet-сервісу користувач може ввійти у комп'ютер провайдера і через нього, з використанням командного shell-режиму, одержати доступ до інших комп'ютерів в Internet.

Крім традиційного застосування, telnet дає змогу приєднатися через нестандартний порт і організувати спеціальну програму-сервер для опрацювання запитів, а також з відлагоджувальною метою увійти в іншу машину через порт іншої програми та дослідити її роботу.

Незважаючи на деяку примітивність інтерфейсу, telnet є важливим базовим інструментом, особливо для досвідчених Unix-користувачів.

Передавання файлів. ftp – це сервіс передавання файлів. Як і telnet, ftp має інтерфейс командного рядка. Структура команди ftp така:

```
% ftp адреса віддаленого комп'ютера.
```


Після того, як виконано сполучення та введено реєстраційну інформацію, користувач з використанням низки простих команд може копіювати файли з віддаленого комп'ютера на свій та навпаки. Головні команди:

```
ftp >get файл_що_читається файл_в_який_передається
ftp >put файл_що_читається файл_в_який_передається
```

Командний режим ftp підтримує і кілька допоміжних команд, які дають змогу переглядати зміст каталогів на віддаленому комп'ютері. Сервіс ftp допускає два режими передавання даних: двійковий (binary) та текстовий (ASCII). Якщо приймання відбувається у двійковому режимі, то файл не опрацьовується і надходить користувачу у первісному вигляді. Якщо ж файл передано у режимі ASCII, він інтерпретується як набір текстових символів з можливістю втрати значення найстаршого біта кожного байта.

Команди mput та mget дають змогу передати або приймати групу файлів, а додаткові команди cd, dir, ls – виконувати навігацію каталогами віддаленого комп'ютера, виводити список файлів каталогу.

Електронна пошта – це базовий, найпростіший і водночас досить потужний сервіс. Він дає змогу пересилати текстові файли за довільною адресою. Адреса в мережі Internet має структуру

```
ім'я_користувача@ім'я_комп'ютера,
```

де ім'я комп'ютера може бути доменним. Інші мережі, до яких Internet приєднана через шлюзи, мають власні системи електронної пошти та формати адрес. На це треба зважати під час пересилання повідомлень у такі мережі.

Листи електронної пошти, подібно до звичайних, передаються через низку проміжних комп'ютерів до адресата. Вислідна швидкість передавання менша, ніж у випадку користування телефоном, і більша, ніж у випадку користування звичайною поштою. Крім пересилання поштових повідомлень, електронна пошта дає змогу організувати роботу групи, створити список розсилання за інтересами, передавати файли тощо.

Кожне поштове повідомлення має заголовок, який містить розділи
- **To:** (Куди);
- **From:** (Звідки);
- **Subject:** (Тема).

Під час проходження повідомлення до заголовка можуть додаватися позначки проміжних пунктів передавання, наприклад, їхні адреси.

Є багато пакетів електронної пошти для різних платформ та з різним сервісом. Базовою та найпростішою можна вважати утиліту *sendmail* ОС Unix (див. розділ 43). Вона дає змогу створювати та надсилати повідомлення, а також виконує інші функції, зокрема створення псевдонімів (замість складної адреси можна набирати короткий та зручний псевдонім). У файлі mailrc у цьому випадку вводять рядок alias псевдонім адреса.

Іншою функцією електронної пошти є організація інформації у вигляді папок та навігація між ними. Крім того, утиліта sendmail дає змогу задавати групи користувачів (вони називаються **списками розсилання**). У файлі mailrc (команда alias) вводиться кілька рядків з однаковим

псевдонімом або замість однієї адреси через кому перелічуються декілька. Коли повідомлення надходить на ім'я псевдоніма, воно пересилається на всі зазначені адреси.

До інших сервісних функцій електронної пошти належать пересилання файлів у двійковому форматі, повідомлення про одержання, повідомлення про прочитання, відміна повідомлення.

Однак пересилання електронною поштою файлів у двійковому форматі є проблематичним. Спочатку пошта була спроектована тільки для пересилання текстової інформації (тобто багато службових символів кодової таблиці були 'нелегальними'). У процесі роботи виникла потреба приєднувати до текстових повідомлень довільні двійкові файли. Їх перекодовували відображенням недопустимих символів у текстові і збільшенням первинного розміру файлу за допомогою утиліт *uuencode/uudecode*. Пізніше був розроблений спеціальний протокол розширення MIME.

Інколи зручно створювати централізований список розсилання на певному сервері і доручити відповідати за нього певному системному адміністратору. Тоді інформація, призначена для групи користувачів, розсилається їм усім. Такі списки називаються **відбивачами пошти**. Як звичайно, відбивачі пошти регулюють передавання інформації групі з певними однаковими інтересами.

Крім того, є спеціальні утиліти *listserv*, *mailserv* та інші, що дають змогу 'передплатити' певний список розсилання або відмінити передплату. Відбивачі пошти можна реалізувати ієрархічно. У цьому випадку обсяг інформації, що передається мережею, зменшиться.

Служби електронної пошти надають послуги і з шукання файлів. Це можна реалізувати одним з трьох способів:

- використанням спеціалізованих серверів Internet;
- використанням списків розсилання listserv, mailserv та ін.;
- використанням спеціалізованих шлюзів FTP/пошта.

Як звичайно, одній із служб спрямовується повідомлення, в тексті якого є команди, що специфікують, які файли треба надіслати. Структура повідомлень та набори команд для кожної служби інші.

Телеконференції. Одним з недоліків використання списків розсилання електронної пошти може стати невиправдане перевантаження мережі. Користувачів можуть не цікавити абсолютно всі повідомлення, які надходять за списком і засмічують поштову скриньку користувача. Можливість ефективно спілкуватися за тематичними інтересами надає сервіс телеконференцій.

Телеконференції – це дискусійні групи з певної тематики. Тематика організована ієрархічно, у вигляді дерева. Тему конференції, наприклад, можна сформулювати так: rec.music.folk (дозвілля.музика.народна). Головні розділи конференцій:

- comp – все про комп'ютери;
- news – новини про систему телеконференцій;
- rec – теми дозвілля, хоббі, мистецтва;
- sci – науково-дослідна діяльність;
- soc – соціальні проблеми;
- talk – дискусії зі спірних питань;
- misc – різне;

- alt – альтернативні погляди на речі;
- k12 – конференція для викладачів і учнів.

З фізичного погляду користувач приєднується до сервера новин, що діє в мережі інших серверів новин, з якими обмінюється інформацією щодо вибраних тем (рис. 31.1). Сервер збирає новини з локальних джерел, з системи новин **USENET**, зі списків розсилання або комерційних систем, таких, як **Clarinet**. Він може вести власні локальні конференції та пропонувати їх іншим серверам. Інформація на сервері затримується протягом визначеного адміністратором часу, а потім архівується та знищується. Сервери телеконференцій використовують спеціальний протокол **NNTP**.

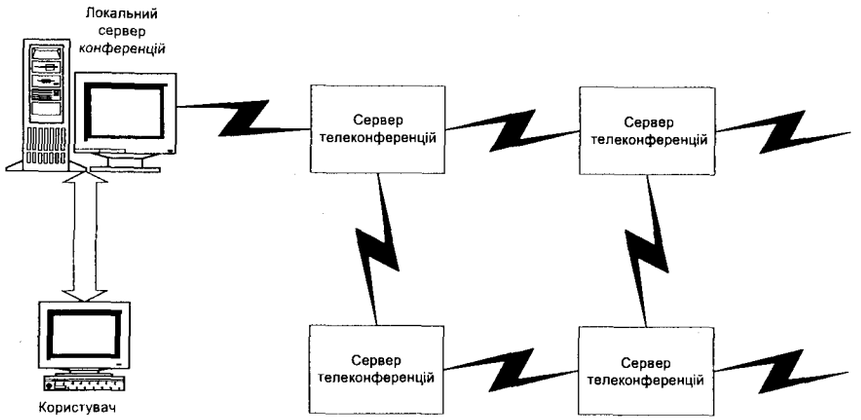


Рис. 31.1. Мережа серверів телеконференцій.

Для роботи з телеконференціями користувач застосовує спеціальну програму (rn, trn, nn, tin), спочатку налагоджуючи конфігураційні файли (наприклад, .nn/init, .newsrc), та зазначаючи, якими конференціями він не буде користуватися та на які зголоситься. Програма роботи з матеріалами конференцій дає змогу зручно переглядати теми окремих повідомлень, самі повідомлення, висловлювати свою думку у відповідь на наявне повідомлення або ж сформувати власне повідомлення на конференцію. Додатковими функціями є фільтрування матеріалів конференцій та тем повідомлень за ключовими словами, шифрування повідомлень, надсилання відповіді автору електронною поштою (у цьому випадку відповідь надходить тільки автору, а не всім учасникам).

Шукання інформації (archie). Серед проблем, з якими стикається користувач Internet, найважчою є відшукання потрібної інформації. Відомо багато різноманітних сервісів шукання, один з них називається **archie**.

У мережі є призначені сервери (як звичайно, їхні імена починаються з archie), які періодично звертаються до серверів Internet свого околу через ftp та читають повну структуру каталогів. Набори структур каталогів різних серверів і формують інформаційну базу, за якою відшукується інформація на підставі імен файлів.

World Wide Web – один з найновіших та найперспективніших сервісів Internet. В основі цієї технології є принцип гіпертексту – гнучкої системи посилань, розташованих у тексті. Такий принцип переходу найбільш відповідає порядку роботи людського мозку під час побудови аналогій та деталізації. Принципи побудови гіпертекстових систем відомі давно. З використанням цієї технології тривалий час створювали help-системи програмних продуктів. Однак уперше гіпертекст для роботи в Internet застосували фізики-ядерники з Європейського центру ядерних досліжень (CERN). Вони розробили web-технологію та створили першу програму перегляду – браузер. Web-технологія відразу ж набула популярності завдяки таким характеристикам:

- інші технології працюють з незручним у користуванні та ненаочним текстовим командним інтерфейсом. Набирання команди займає багато часу. Посилання WWW не потребують набирання взагалі;
- графічний інтерфейс. Переважна більшість програм перегляду – графічні;
- єдина програма для виконання всіх функцій – браузер. Програма проста у користуванні;
- механізм гіпертекстових переходів дає змогу зручно впорядкувати інформацію;
- підтримує відображення мультимедіа інформації;
- підтримує доступ до баз даних;
- зручний доступ до всіх інших сервісів Internet з браузера;
- можливість багатовіконної роботи з кількома документами.

Для передавання Web-документів використовують протокол **HTTP** (Hypertext Transfer Protocol). Web-технологія має уніфікований механізм зображення адреси мережевого ресурсу **URL** (Uniform Resource Locator). Форми URL для деяких сервісів WWW наведені в таблиці.

Таблиця 31.1. Форми URL для деяких сервісів WWW

Сервіс	URL
www	http://internet_адреса/шлях_до_файлу_html
ftp	file:// internet_адреса/шлях_до_файлу
telnet	telnet:// internet_адреса:порт
телеконференції	news://назва_конференції

Web-документи створюють спеціальною мовою, що враховує гіпертекстові посилання, мультимедіа інформацію тощо, – **HTML** (Hypertext Markup Language). Формат текстового файлу web-документа – html. Крім статичних web-документів, можуть бути і динамічні. Їх формує web-сервер автоматично на підставі інформації з баз даних та передає користувачу. Такі документи повинні відповідати специфікації **CGI** (Common Gateway Interface).

Бібліографія та джерела

Крол Э. Все об Internet. К.: BHV. 1995.

ВІДКРИТІ СИСТЕМИ

Поняття 'відкрита система'. Вимоги до відкритих систем. Стандарти POSIX. Модель компонент відкритого середовища. Фактори, що обмежують впровадження відкритих систем. Архітектурний підхід до розробки систем.

Серед багатьох чинників, які визначали мету розвитку мережевих інформаційних систем, найбільше значення мало поняття *відкриті системи.* У розділі 2 наведено означення відкритих систем як таких, що реалізовані згідно з міжнародними стандартами. Розглянемо проблематику відкритих систем детальніше.

У літературі є різноманітні означення та тлумачення поняття **відкритої системи**. Мабуть, жоден з виробників обладнання чи програмного забезпечення не погодиться, що його продукт не є 'відкритим'. Водночас ці ж виробники переконано доводять, що серед продуктів конкурентів багато таких, які з великим перебільшенням можна віднести до відкритих.

Однією з груп міжнародних організацій, що вивчають та визначають поняття відкритої системи, є група розробки стандарту інтерфейсу переносних операційних систем (Portable Operating System Interface (POSIX)) IEEE. Згідно з означенням групи IEEE P1003 відкрита система *реалізує достатньо відкриті специфікації для інтерфейсів, сервісів та форматів, щоб дати змогу коректно спроектованому застосуванню:*

- *переноситись через велику кількість систем з мінімальними змінами;*
- *взаємодіяти з іншими застосуваннями у локальних та віддалених системах;*
- *взаємодіяти з користувачем у стилі, який полегшує перенесення користувача.*

Дуже часто, особливо прихильники ОС Unix, назву цієї ОС використовують як синонім відкритої системи. Проте поняття відкритої системи є значно ширшим.

Отже, центральне поняття відкритих систем – це поняття відкритого стандарту, що є певною відкритою функціональною специфікацією. IEEE P1003 визначає відкриту специфікацію як *загальнодоступну, яка підтримують відкритим, загальним процесом досягнення консенсусу для реалізації нової технології у часі і яка сумісна з міжнародними стандартами.* У такому формулюванні наявність відкритих стандартів визначається процесом їхньої постійної підтримки всіма зацікавленими сторонами. На думку фахівців, обов'язкові вимоги до продукту, який має відкриту специфікацію, такі:

- **масштабованість** (Scalability) – незалежність від апаратного забезпечення під час перенесення з малих на середні та великі системи;
- **здатність взаємодіяти** (Interoperability) – можливість обміну інформацією з іншими системами та її сумісне використання;
- **цілісність, послідовність** (Consistency) – однаковий, логічно цілісний та послідовний інтерфейс користувача на всіх платформах, де застосовують систему;

• **супровід** (Maintenance) – специфікація повинна допускати процес відкритого супроводу усіма зацікавленими сторонами;

• **переносність** (Portability) – систему можна легко переносити на різні апаратні та програмні платформи.

Зрозуміло, що проблематика відкритих систем не обмежується лише операційними системами чи стандартами з передавання даних. Вона охоплює всі аспекти функціонування інформаційної системи. Однією з моделей, що повинні охопити головні компоненти побудови відкритого інформаційного середовища, є модель, розроблена Центральною агенцією з питань комп'ютерів та телекомунікацій (Central Computer and Telecomunications Agency (CCTA)) у Великобританії. Для полегшення запам'ятовування використовують акронім **MUSIC**:

• **M – Management**. Стандарти щодо керування інформаційними ресурсами дають змогу мережевим адміністраторам взаємодіяти, конфігурувати параметри систем, а також взаємодіяти самим системам;

• **U – User Interface**. Стандарти щодо користувацького інтерфейсу передбачають подібний вигляд елементів інтерфейсу, порядок їх взаємодії з користувачем;

• **S – Systems and applications Interface**. Передбачають стандартизацію мов запиту до інформаційних ресурсів (наприклад, SQL), інтерфейсів програмування (API), що регламентують доступ до системних функцій;

• **I – Information and data services**. Стандарти охоплюють формати даних, у тому числі двійкові. Вони дають змогу одні й ті ж дані використовувати в різних системах. Сюди також належать об'єктно-орієнтовані мови програмування, Java та архітектури розподілених обчислень;

• **C – Communication Services**. Власне мережеві стандарти, що дають змогу взаємодіяти мережевому обладнанню незалежно від користувача, надавати телекомунікаційні послуги незалежно від абонентів.

Вигода від відкритості інформаційних систем така. В умовах наявності багатьох виробників-конкурентів відкриті системи більш гнучкі. Вони дають змогу вибрати найліпші продукти різних виробників та спроектувати з них одну систему. Дотримання стандартів зменшує час розробки системи, навчання користувачів, витрати на керування, адміністрування та діагностику. Однак впровадження відкритості у світ інформаційних систем гальмують такі фактори:

• наявність великої кількості застарілих систем та застосувань (legacy systems). У них свого часу вкладено значні інвестиції, вони підтримують виробничі процеси, і користувачі не хочуть відмовлятися від них повністю. Водночас понад 80% ресурсів йде на підтримку цих систем. Найновіші технології, як звичайно, використані у невеликій кількості застосувань;

• переносність систем обмежується попередніми інвестиціями в непереносний код, у навчання персоналу, у встановлені бази даних.

Водночас і самі стандарти мають такі обмеження:

• вони неповні, що дає окремим виробникам широке поле для розробки власних, несумісних вирішень;

• наявні стандарти не завжди правильно передбачають розвиток технологій у майбутньому. Окремі вже стандартизовані вирішення можуть стати гальмівним фактором.

Яким же чином провідні фірми вирішують проблему розвитку своїх продуктів в умовах, коли:

• нема єдиних стандартів на всі компоненти систем;

• передові апаратно-технічні та програмні вирішення постійно змінюються;

• у наявні, можливо, застарілі вирішення та інфраструктури вкладено великі кошти;

• старі системи працюють, у їхніх базах даних накопичено багато важливої інформації і відмова від таких систем недопустима;

• кожна фірма вважає, що випускає 'відкриті' продукти?

На думку фірми DEC (Digital Equipment Corporation), вихід полягає у використанні для визначення технічної політики архітектурного підходу.

Архітектура в такому розумінні – *це комплекс стратегічних вирішень з розробки продукту або серії продуктів, який дає змогу всім частинам розробки взаємодіяти та розвиватися у часі.*

Правильна архітектура – це своєрідний план на майбутнє з усіма частинами, спроектованими так, щоб з самого початку працювати, взаємодіяти та змінюватися. Система, спроектована з дотриманням архітектурного підходу, дає змогу змінювати одну частину без зміни інших.

Бібліографія та джерела

Guide to information systems: a framework for success. DEC: Educational Services Media Comunications, 1995.

Частина 3

ОПЕРАЦІЙНІ СИСТЕМИ КОМП'ЮТЕРНИХ МЕРЕЖ

ПРИНЦИПИ ОРГАНІЗАЦІЇ ОПЕРАЦІЙНИХ СИСТЕМ КМ

Призначення ОС КМ. Сервери. Робочі станції. Типи серверів. Класифікація ОС КМ. Загальна схема операційної системи КМ. Програма переспрямування. Особливості апаратно-програмних вирішень файл-сервера. Паралельне опрацювання інформації. Особливості роботи сервера друкування.

Центральне місце в комп'ютерній мережі посідає мережева операційна система. Вона дає змогу об'єднати різне комунікаційне та інформаційно-обчислювальне обладнання в єдиний робочий комплекс – комп'ютерну мережу.

Мережева ОС дає змогу користувачу спільно використовувати:

• дорогі апаратні ресурси мережі – потужні (heavy duty) принтери, сканери, дискові накопичувачі, інше цінне периферійне обладнання;

• програмне забезпечення, коли ПЗ інсталюють тільки в одному примірнику і застосовують усі користувачі мережі;

• інформаційні ресурси, цінні бази даних. Інформацію змінюють в одному місці й використовують усі користувачі;

• організувати сумісну роботу великого колективу користувачів з оперативним обміном інформацією між ними.

33.1. Складові частини КМ та ОС

Комп'ютери мережі відповідно до функцій та ресурсів, які вони виділяють для загального користування, поділяють на такі.

Сервери – це комп'ютери, які надають частину своїх ресурсів для загального користування абонентам мережі. Вони бувають різні. Залежно від типу ресурсу є файл-сервери, сервери друкування, модем-сервери та ін. Файл-сервери виділяють свій дисковий простір та файли для загального користування та керують цим процесом. Сервери друкування керують друкуванням на мережевому друкарському пристрої, на який надходять завдання зі всієї мережі. Сервери також бувають *призначеними (dedicated)* та *непризначеними (non dedicated)*. Призначені сервери займаються тільки організацією обслуговування запитів, що надходять з мережі, а непризначені, крім того, працюють зі своєю прикладною програмою і користувачем. Непризначений сервер менш надійний: прикладна програма користувача на ньому може призвести до його 'зависання'. Через це сервер припинить роботу усієї мережі.

Робочі станції – це комп'ютери, що використовують ресурси, надані серверами, проте своїх ресурсів для користування не виділяють.

В адаптерах мережі апаратно реалізовані протоколи фізичного та канального рівнів. Функції протоколів верхніх рівнів та деякі адміністративні виконує операційна система мережі.

33.2. Класифікація ОС КМ

Залежно від набору класифікаційних ознак ОС та побудовані на їхній основі КМ поділяють так.

За наявністю призначених серверів:

• **однорангові** (peer to peer). Кожна робоча станція може одночасно бути сервером та робочою станцією. Такі системи гнучкіші. Вони особливо вигідні для організації робочих груп (приблизно до 20 станцій). Недоліки: складність адміністрування у великих мережах, менша надійність;

• **з окремими серверами**. Для виконання серверних функцій виділяють окремі машини. На них встановлюють системне програмне забезпечення, спроектоване спеціально для виконання серверних функцій. Сервери можуть бути призначені (наприклад, у Netware 4.x) або непризначені (наприклад, у MS Windows NT).

За характером роботи:

• ті, що працюють у режимі витіснення. Спеціальний диспетчер виділяє процесам кванти часу центрального процесора (Unix, Windows 95, Windows NT);

• ті, що не працюють у режимі витіснення. Процеси самі віддають керування іншим процесам (Netware).

33.3. Структурна схема та головні функції операційної системи КМ

Операційна система мережі складається з серверних компонент та компонент операційної системи на робочих станціях. Спрощена структура ОС показана на рис. 33.1.

В основі операційних систем робочих станцій є проста *програма переспрямування (redirector)*. Вона резидентно міститься в пам'яті комп'ютера. Коли користувач або його програма звертаються з запитом до операційної системи комп'ютера, ця програма 'перехоплює' запит, аналізує, хто його може виконати, і спрямовує або в ОС тієї ж машини, або в сервер, якому адресовано цей запит. Користувач не бачить, до яких ресурсів (своєї машини чи мережі) він звертається. Програма переспрямування зберігає інформацію про наявність серверів мережі і ставить у відповідність символьним посиланням (наприклад, a:, o:, z:, lpt1:) реальні ресурси локального комп'ютера або мережі. На відміну від багатотермінальної системи, завдання в КМ виконуються на робочих станціях та читаються з файл-сервера.

Ідею переспрямування широко застосовують в архітектурі сучасних мережевих ОС головним чином для збільшення універсальності їх застосування, наприклад, в організації багатопротокольності (див. розділ 45).

Операційна система сервера складніша. Вона виконує набір функцій, які можна розділити на такі групи:

• підтримка файлової системи;

- керування пам'яттю;
- планування завдань;
- адміністративні функції;
- керування друкуванням.

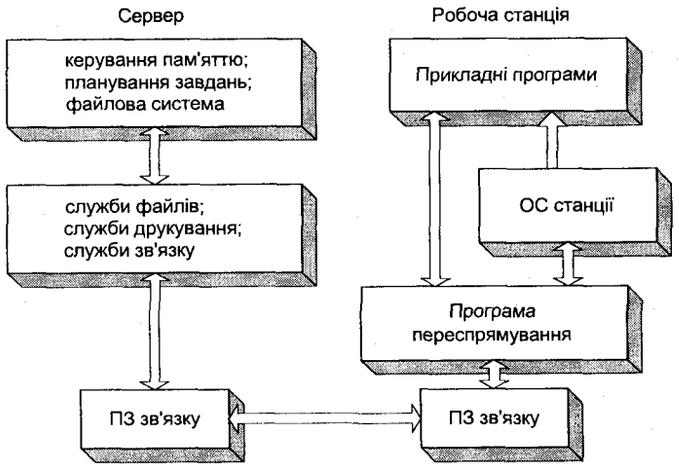


Рис. 33.1. Структурна схема ОС мережі.

Конкретний набір функцій сервера залежить від типу сервера та його конфігурації. Наприклад, для файл-сервера головними є функції файлової системи, планування завдань, керування пам'яттю та доступом до ресурсів. До появи ідеології файл-серверів кожен користувач прямо звертався до диска так званого диск-сервера. Оскільки вплив перешкод від одночасного звертання був значним, то така система не була надійною і не зберігала цілісність інформації. У файл-сервері запит спочатку потрапляє в ОС сервера, яка керує доступом усіх користувачів та дає змогу уникнути взаємних перешкод.

ОС сервера, що працює з DOS, застосовує деякі вбудовані в цю ОС функції, орієнтовані на колективне використання файлів, зокрема розширене відкривання файлів та їхнє фізичне блокування. Функція розширеного відкривання визначає, які права доступу можуть мати користувачі, а саме: читання, записування, читання/записування. Якщо файл потрібно змінити, то його відкривають з правом читання/записування та відміняють такі права для інших користувачів. Права зберігають аж до закриття файлу. Описане відкривання файлу називається *неподільним (монопольним)*. Якщо файл треба читати, то його можна відкрити з правом читання та заборонити записування для інших. Файл можуть відкрити одночасно кілька користувачів, якщо їхні права не суперечать одне одному. Якщо два або більше користувачів одночасно хочуть змінити файл, то ОС використовує операцію блокування запису. Прикладні програми можуть блокувати конкретний запис. Отже, однією з функцій ОС мережі є керування доступом до файлів, створення черг запитів та керування ними. Іноді реалізується пріоритетний доступ до

файлів. Концепцію спільного використання файлів найзручніше описати на прикладі операцій з базами даних.

Спеціальні операції керування колективним доступом до баз даних є практично в усіх СКБД. У деяких з них (Access, Foxpro, Oracle, Informix, Sybase) блокування записів відбувається автоматично, в інших це робить програміст. Команди СКБД дають змогу відкривати всі бази в монопольному режимі:

```
SET EXCLUSIVE ON,
```

або тільки одну конкретну базу:

```
USE <database> EXCLUSIVE.
```

У такому випадку аж до закриття бази командою

```
CLOSE
```

нею може користуватися тільки один користувач.

Якщо режим монопольного використання не заданий, можна блокувати активний запис функціями

```
FLOCK(), RLOCK().
```

Файл-сервер також виконує функцію керування повноваженнями. Кожному файлу або каталогу ставиться у відповідність список користувачів, які мають доступ до нього, та тип цього доступу.

33.4. Особливості апаратно-програмних вирішень файл-сервера

Комп'ютер файл-сервера посідає особливе місце серед інших комп'ютерів мережі. Він повинен мати більші ємності для зберігання даних, більші швидкодію та оперативну пам'ять.

Критичним моментом у роботі файл-сервера є його здатність швидко відшукувати дані та видавати їх без помітної затримки робочій станції. На продуктивність файл-сервера впливають багато факторів: швидкість роботи адаптера, тип мережі, ємність доступної оперативної пам'яті, параметри твердого диска. Найважливішим параметром файл-сервера є час доступу до даних. Він складається з часу шукання (радіального переміщення головок) та часу обертання (часу, потрібного для підходу потрібного сектора). Добрим є сервер з часом доступу 10–25 мс. Збільшити продуктивність файл-сервера та надійність зберігання даних можна за допомогою різних апаратних та програмних вирішень. Назвемо деякі з них.

Використання дискового співпроцесора. Спеціальний дисковий співпроцесор керує читанням та записуванням інформації на диск. Отже, розвантажується центральний процесор, збільшуються продуктивність та вартість системи.

Застосування інтелектуальних адаптерів. Частину роботи щодо організації обміну даними та доступу до пам'яті виконує адаптер, використуючи спеціальні алгоритми. Як

звичайно, адаптери серверів коштують дорожче. Крім того, вони можуть мати більшу розрядність або використовувати прямий доступ до пам'яті.

Ліфтове шукання (elevator seeking). Ліфтове переміщення головок дисковода – це процедура, що дає змогу поліпшити записування та читання даних з диска. Запити, які надходять, накопичуються протягом деякого часу. Після цього оптимізується їхня черговість, щоб мінімізувати переміщення головок. Така процедура зменшує тривалість виконання запиту на 40%. Крім того, зменшується зношування диска.

Кеш-пам'ять (cash memory). На сервері розміщують спеціальну швидкодіючу пам'ять, у яку заносять структуру каталогів та FAT-таблиці (апаратний кеш). Крім того, частину вільної оперативної пам'яті комп'ютера виділяють для читання/записування. Кожного разу читають не тільки визначений кластер диска, але й кілька сусідніх (файли найчастіше містяться в сусідніх кластерах). У цьому випадку велика ймовірність того, що наступне читання можна буде виконати з пам'яті, а не з диска. Отже, тривалість доступу зменшиться.

Кешування файлів. У процесі роботи система може аналізувати, які файли використовуються найчастіше, та зберігати їх у пам'яті, а не на диску. Це разом з операцією ліфтового шукання підвищує ефективність застосування сервера в сотні разів.

Гешування каталогів (directory hashing). Якщо каталоги в сервері дуже великі, то потрібен тривалий час на відшукання конкретного файлу за його іменем (необхідно переглянути всі імена попередніх файлів каталогу). У процесі гешування кожен запис каталогу перетворюється у 2-байтові значення, які зберігаються в спеціальних геш-таблицях. Шукання потрібного імені файлу зводиться до порівнянь числових значень з цих таблиць.

Індексування FAT- та геш-таблиць. Для прискорення шукання застосовують індексування таблиць. У цьому випадку створюють та зберігають спеціальні індексні файли.

Дублювання дисків (disc mirroring). Поряд з одним встановлюють другий ідентичний твердий диск, який в оперативному режимі дублює роботу першого. Якщо один вийшов з ладу, робота сервера не припиняється.

Мультипроцесорність. Для збільшення швидкодії в сучасних серверах щораз частіше використовують кілька (до кількох десятків) процесорів, які працюють у режимі розподілу пам'яті (Symmetrical Multiprocessing (SMP), Asymmetrical Multiprocessing (ASMP)). Як звичайно, у таких серверах можна виконати гарячу (без припинення роботи сервера) заміну окремих блоків (див. Д.33.1).

RAID-масиви. У сучасних серверах для збільшення гнучкості, надійності зберігання та обсягів інформації часто використовують масиви твердих дисків.

33.5. Особливості реалізації та роботи сервера друкування

Сервер друкування – це комп'ютер, який виконує завдання для окремої групи користувачів з друкування матеріалів. Як звичайно, він керує одним або кількома принтерами. Подібно до файл-сервера, сервер друкування може бути призначеним та непризначеним.

Якщо якійсь робочій станції дано завдання роздрукувати документ, то вона звертається до принтера мережі за його символьним іменем (до робочої станції можна приєднати і локальний принтер, однак він повинен мати інше ім'я). Програма переспрямування, в якій зберігається інформація про ресурси мережі, надсилає запит до сервера друкування. Якщо принтер вільний, сервер відразу спрямовує завдання в буфер друкування – частину оперативної пам'яті сервера, яка використовується для скерування завдань на друкування з заданою швидкістю (рис. 33.2).

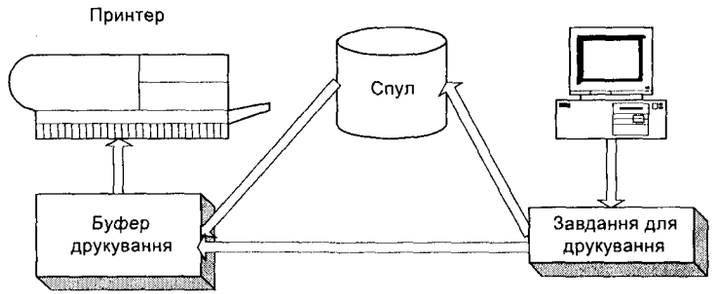


Рис. 33.2. Робота сервера друкування.

Якщо принтер зайнятий, то завдання записується на диск сервера друкування і чекає своєї черги. Програмне забезпечення сервера друкування може керувати чергою, присвоювати завданням пріоритети, групувати за форматами документів та ін. Якщо буфер друкування частково звільняється, до нього надходять завдання з диска. Такий процес називається *спулінгом (spooling)*, відповідний програмно-апаратний механізм – *спулом друкування*.

Бібліографія та джерела

1. Организация локальных сетей на базе персональных компьютеров. М.: ИВК-СОФТ, 1991.
2. *Пенрод Д.* Netware: поворот к мультипроцессорной обработке // Сети. 1995. № 2.
3. *Титтел Э., Коннор Д.* Netware для чайников.К.: Диалектика, 1995.
4. *Фролов А.В., Фролов Г.В.* Локальные сети персональных компьютеров. Монтаж сети, установка программного обеспечения. М.: ДИАЛОГ-МИФИ, 1995.
5. Oracle Parallel Server in the Digital Environment. Oracle White paper, 1997.

ДОДАТКИ ДО РОЗДІЛУ 33

Д.33.1. Паралельне опрацювання інформації

Паралельне опрацювання інформації – підхід, який дасть змогу суттєво збільшити надійність надання інформаційних послуг та зменшити час обслуговування клієнта сервером. Сьогодні є декілька варіантів такого підходу.

З погляду організації використання пам'яті процесорами розрізняють симетричне та асиметричне мультипроцесування.

• **Симетричне мультинроцесорне опрацювання** (SMP) застосовують на стандартних комп'ютерах з кількома процесорами (2–6). Процесори використовують спільний масив пам'яті і спеціальні процедури узгодження її використання. SMP дає змогу значно прискорити опрацювання інформації. Його використовують на стандартних універсальних комп'ютерах, однак суттєвого поліпшення надійності воно не дає. Якщо вийшла з ладу компонента комп'ютера, обслуговування клієнтів припиняється. Покращеним варіантом архітектури SMP є архітектура NUMA (див. Д.33.2).

• **Асиметричне мультипроцесорне опрацювання** (ASMP). На багатопроцесорній машині кожен процесор має свою окрему фізичну пам'ять. Процесори узгоджують свою роботу шляхом обміну повідомленнями. У такій системі нема координаційних механізмів використання пам'яті, подібних до механізмів SMP. Надійність та готовність може бути дещо вищою, ніж у SMP-системах, особливо, якщо окремі процесорні блоки незалежні і допускають заміну в гарячому режимі.

Підходи до реалізації одночасного виконання програм у комп'ютерних системах можуть бути такі.

• **Багатопроцесорні універсальні комп'ютери** (у тому числі й персональні), оснащені кількома процесорами (2–6), що працюють у SMP-режимі. На таких комп'ютерах функціонують операційні системи загального використання.

• **Використання дублювання** (mirroring) твердих дисків або цілих комп'ютерів. Диски чи сервери одночасно виконують одні й ті ж операції, повністю дублюючи один одного. Якщо один з серверів чи дисків вийде з ладу, інший продовжить роботу – інформація не буде втрачена і суттєвої перерви в обслуговуванні клієнтів не буде. Такий підхід дає змогу суттєво збільшити надійність конфігурації. Водночас він є найдорожчим і неефективно використовує комп'ютерні ресурси.

• **Застосування спеціалізованих багатопроцесорних машин** (Massively Parallel Processing (**MPP**)). Дуже часто спеціалізація обмежується певним класом задач чи взагалі окремою задачею. Обчислювальні простої MPP будують під конкретне замовлення, тому вони коштують дуже дорого. MPP-системи можна будувати з застосуванням як SMP-, так і ASMP-підходів до використання пам'яті.

• **Застосування кластерних вирішень** (loosely coupled clusters). Окремі комп'ютери (у тому числі з SMP чи ASMP) пов'язують у єдину структуру – кластер. Навантаження розподілене між комп'ютерами. У нормальній ситуації кожен з комп'ютерів виконує свою конкретну роботу. Якщо ж якийсь комп'ютер вийде з ладу, його роботу почне виконувати інший. Є два варіанти реалізації кластера (див. рис. Д. 33.1.1, Д.33.1.2).

У першому варіанті комп'ютери мають спільний дисковий пристрій (приєднаний через SCSI-інтерфейс). Комп'ютери узгоджують свою діяльність шляхом обміну повідомленнями через швидкісну (одну або декілька) мережу (як мережу використовують Fast Ethernet або Fiber Channel). Кожен з комп'ютерів періодично з'ясовує, чи працює інший комп'ютер кластера (наприклад, за допомогою спеціальної heartbeat-процедури). Якщо один з комп'ютерів кластера вийшов з ладу, то на іншому запускаються процедури поновлення з останньої контрольної точки. Залежно від причини відмови комп'ютер може виконувати різні командні файли. Відміняються усі незавершені транзакції. Навантаження з комп'ютера, що вийшов з ладу, переходить на комп'ютер, який працює. На це потрібен деякий час, що впливає на якість обслуговування клієнтів.

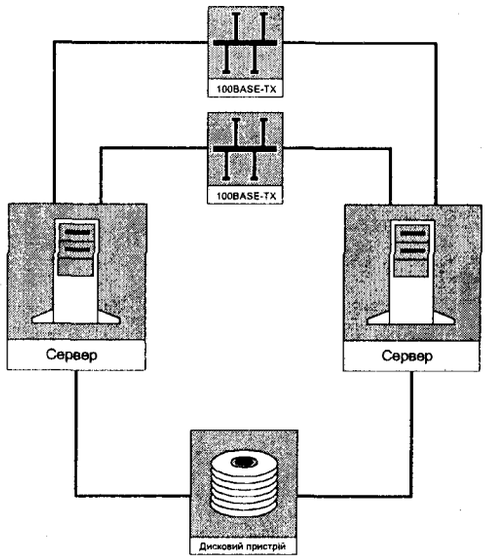


Рис. Д.33.1.1. Кластер з мережевим сполученням.

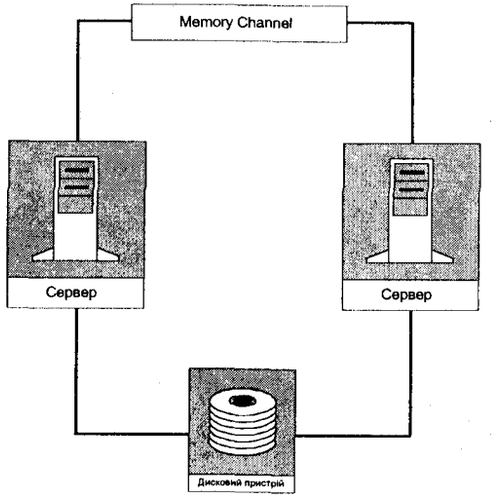


Рис. Д.33.1.2. Кластер архітектури Memory Channel.

Передавання інформації локальною мережею не завжди ефективно використовує перепускну здатність. (Наприклад, під час роботи з базою даних і в разі потреби узгодження цілісності даних, реєстрації транзакції комп'ютери обмінюються невеликими інформаційними повідомленнями.

Під час передавання цих повідомлень мережею їх опрацьовує протокольне мережеве забезпечення усіх рівнів, що призводить до невиправданих витрат ресурсів та значних затримок).

Другий варіант передбачає сполучення комп'ютерів не мережею, а через спеціалізовані адаптери напряму з використанням прямого доступу до пам'яті (DMA). Комп'ютери кластера мають спільний віртуальний простір пам'яті, що дає змогу досягти швидкостей обміну даними, які більші, ніж у першому варіанті, у 10 разів. Подібний підхід, наприклад, використано в розробці фірми Digital *Memory Channel*.

Використання кластерного вирішення дає змогу підвищити як швидкодію, так і готовність системи.

Д.33.2. Мультипроцесорна архітектура NUMA

В архітектурі SMP процесори використовують спільний масив пам'яті та обмінюються інформацією по одній спільній шині. Не дивно, що застосування, які використовують SMP, добре масштабуються тільки до восьми процесорів. З подальшим збільшенням кількості процесорів виграш у продуктивності зменшується, оскільки вузьким місцем системи стають спільні шина та пам'ять.

Архітектуру **NUMA** (Non-Uniform Memory Access) можна трактувати як розвиток архітектури SMP. Якщо в SMP процесори мали спільну пам'ять та шину, то в NUMA вони розділені на групи. Процесори кожної групи мають власний масив пам'яті та обмінюються інформацією по окремій шині. Головна перевага систем з архітектурою NUMA – ліпша масштабованість. (рис. Д.33.2.1).

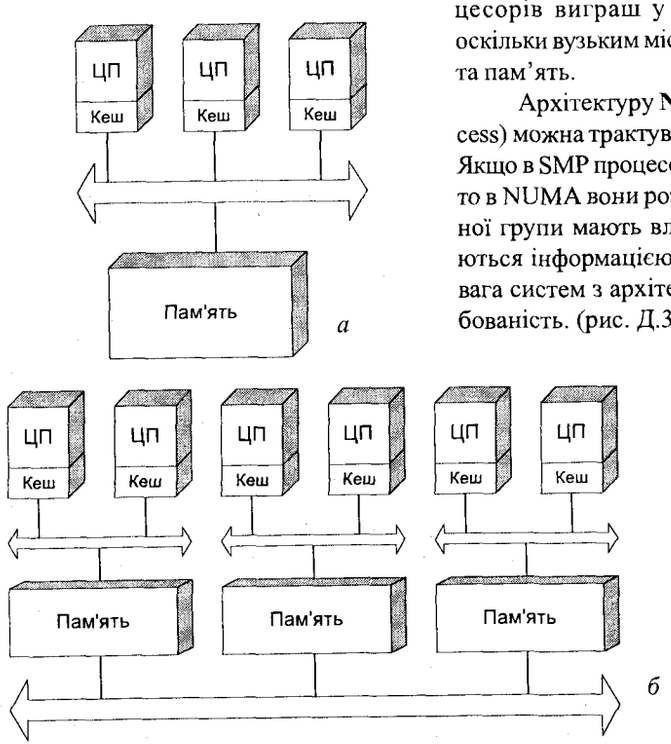


Рис. Д.33.2.1. Архітектури SMP (*а*) та NUMA (*б*).

МЕРЕЖЕВІ АСПЕКТИ WINDOWS 95, 98

Розділ 34

Загальна характеристика та функціональні можливості. Мережеві компоненти. Системна архітектура. Інсталювання та налагодження. Засоби автоматизації інсталювання. Робота в мережі. Механізми обмеження доступу. Робота з системним реєстром. Користувацькі профілі. Системні правила та робота з ними. Віддалене керування. Електронна пошта. Microsoft Exchange та Microsoft Fax. Віддалений доступ.

Мережа ОС Windows 95 належить до однорангових мереж. До цього класу, як звичайно, відносять малі ЛМ з 3–50-ма комп'ютерами. У основі таких ЛМ є концепція робочих груп, згідно з якою кожен власник комп'ютера сам вирішує, які ресурси виділити для загального користування.

Одноранговими ОС є також Lansmart, Lantastic, Windows 3.11.

34.1. Загальна характеристика та функціональні можливості. Мережеві компоненти

Операційна система Windows 95 (W95) має значно розвинутіші мережеві функції порівняно з її попередницями. Її розробники намагалися створити найсучаснішу мережеву ОС, яка б задовольняла такі головні вимоги до сучасних ОС:

- була проста в керуванні, щоб з нею могли працювати малокваліфіковані користувачі;
- підтримувала максимальну кількість протоколів та взаємодіяла з багатьма мережевими ОС; була універсальною;
- поєднувала зручність та простоту адміністрування з розвинутими адмінфункціями та можливістю адміністрування мереж, що об'єднують тисячі комп'ютерів (зменшення витрат на адміністрування);
- мала вбудовану електронну пошту та інші засоби колективної роботи і вихід у глобальні мережі;
- підтримувала віддалений доступ, мобільних користувачів.

W95 – це однорангова ОС, яка передбачає приєднання до серверів Windows NT та Novell Netware. Нижче описано нові вирішення, впроваджені в ОС КМ завдяки розробці W95.

У системній архітектурі. Багатомодульна архітектура, яку налагоджують для підтримки різноманітних функцій за бажанням користувача відповідним набором модулів. Підтримка багатопротокольності.

У засобах керування системними параметрами. Збереження системної інформації в єдиній базі даних – системному реєстрі. Поділ цієї бази на користувацьку та машинну

компоненти, що дає змогу однаково обслуговувати користувача незалежно від місця його входження у мережу. Прості та наочні засоби роботи з реєстром.

У засобах інсталювання. Можна автоматизувати процес інсталювання, створити спеціальні сценарії, інсталювати велику кількість копій ОС без втручання оператора. Налагодження функціональності системи з урахуванням потреб окремих користувачів та їхніх груп.

У засобах взаємодії з іншими системами. Крім підтримки одноранговості, змога бути клієнтом для систем Windows NT та Novell Netware, сервером для клієнтів Windows NT та Novell Netware. Додаткове приєднання до інших серверів. Уніфікація механізму таких приєднань.

У засобах адміністрування. Можна налагоджувати робоче середовище для різних користувачів та їхніх груп (профілі користувачів). Підтримка індивідуального списку паролів доступу до різних ресурсів. Користувач вводить пароль лише один раз – під час входження у систему. Він може входити в мережу з різних комп'ютерів і користуватися одними профілями (робоче середовище переходить за користувачем у разі його переміщення). Можна створювати обов'язкові профілі, а також використовувати системні правила для окремих користувачів та їхніх груп з метою обмеження свободи змін системних параметрів на робочих місцях.

У системі електронної пошти. Система електронної пошти інтегрована в ОС. Це означає, що є єдиний клієнт електронної пошти, який обслуговує як локальну пошту, так і вихід у зовнішні мережі. Він підтримує додаткові споріднені служби (наприклад, передавання факсів). Така інтегрованість електронної пошти дає змогу використовувати її прямо з застосувань.

У підтримці віддаленого доступу. Реалізація головних протоколів віддаленого доступу. Наявність утиліт синхронізації каталогів.

Поряд з перевагами, W95 має і низку недоліків. Зокрема, підтримує тільки застарілу версію Novell Netware (без змоги працювати з деревом каталогів). Є недоліки в механізмі захисту системи.

Для зручності користувача ОС та структурування мережевих функцій у W95 виділені такі типи мережевих компонент.

- **Мережевий адаптер.** Ця компонента містить як параметри реального мережевого адаптера, так і протоколів PPP, SLIP. Одночасно можна сконфігурувати кілька адаптерів.
- **Протокол.** Як звичайно – це визначення певних протокольних стеків (SPX/IPX, Microsoft DLC, NETBEUI, TCP/IP). Протоколи 'прикріплюються' до адаптерів та мережевих клієнтів. Одночасно може підтримуватись кілька протокольних стеків.
- **Клієнт.** Мережевий клієнт дає змогу сполучатися з серверами відповідних мереж. Допускається встановлення клієнтів Banyan, FTP Software, Microsoft, Novell, Sunsoft. Клієнти Microsoft, Novell не потребують додаткового ПЗ.
- **Служба.** Мережева служба – це сукупність засобів, які виконують певну мережеву функцію. Наприклад, *Служба доступу до файлів та принтерів*. Окремо визначені такі служби для мереж Microsoft та Novell.

34.2. Мережева архітектура

Архітектура W95 побудована на моделі взаємодії відкритих систем ISO. Вона має модульну структуру, що ґрунтується на специфікації **WOSA** (Windows Open Services Architecture). Модульна структура забезпечує гнучкість, легкість у налагодженні та керуванні, зменшення розміру коду та підвищення швидкодії. Структура W95 відкрита та дає змогу розробникам інших фірм створювати програми взаємодії (рис. 34.1).

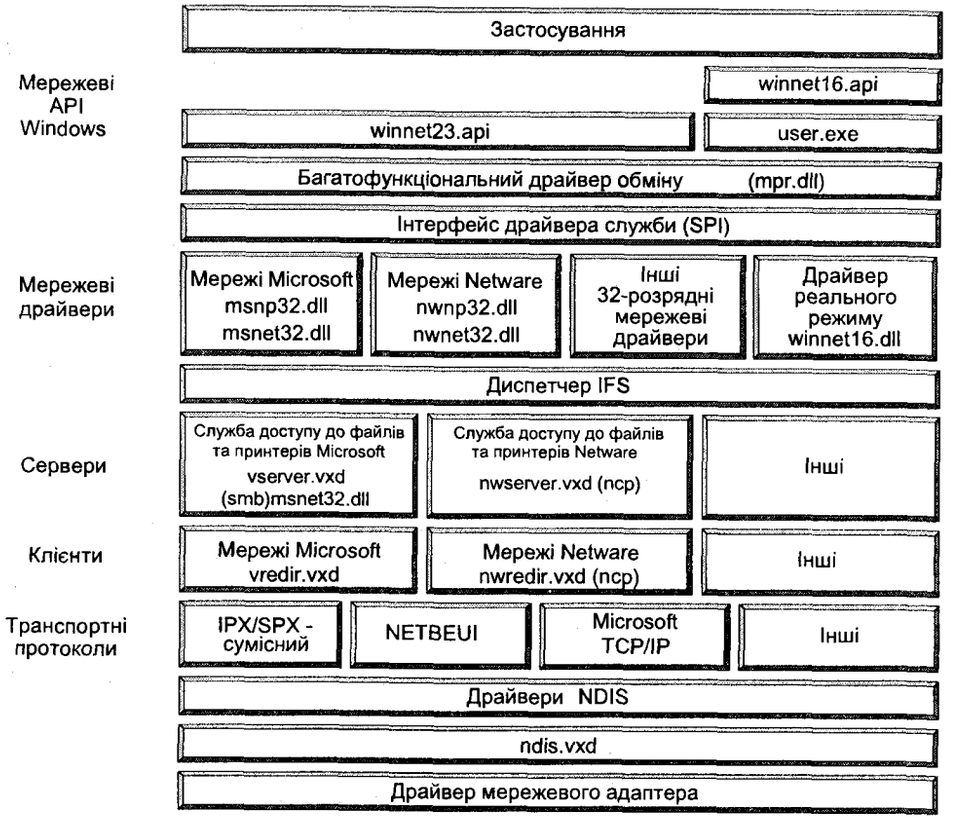


Рис. 34.1. Мережева архітектура W95.

Верхнім рівнем архітектури є *застосування Windows*. Вони взаємодіють з мережевими функціями за допомогою декількох *мережевих API (Application Program Interface)* стандартизованих наборів функцій та процедур, які можна викликати з програм-застосувань. Усі мережеві операції застосувань можуть відбуватися тільки через ці функції. Є такі API:

• *WinNet32* – головний мережевий API. Містить 32-розрядні функції. Підтримка всіх типів мереж та протоколів. Можна створювати застосування незалежно від типів мереж;

• *WinNet16* – незалежне від типу мережі 16-розрядне API, яке використовують у Windows 3.1;

• *Windows Sockets* – набір функцій для забезпечення інтерфейсу між Windows та застосуваннями, що створені для протоколу TCP/IP. Практично всі Internet-орієнтовані Windows-застосування написані з використанням цього інтерфейсу. Windows Sockets, окрім TCP/IP, підтримує і протокол SPX/IPX.

W95 має елементи, що дають змогу підтримувати декілька мереж одночасно. З ними можна працювати за допомогою 32-розрядних програмних модулів, розроблених для роботи у захищеному режимі. Дозволена робота одного 16-розрядного модуля реального режиму. W95 має клієнтські модулі таких ОС: Artisoft Lantastic v.5.0, Banyan Vines v.5.2, DEC Pathworks, Novell Netware, SunSoft PC-NFS v.5.0. Підтримуються також усі наступні версії.

Багатофункціональний драйвер обміну ***MPR*** *(Miltiple Provider Router)* – це редиректор, що переспрямовує інформацію від мережевого API відповідним мережевим драйверам. Драйвер обміну реалізовано як файл mpr.dll. У ньому є спільний для мережевих драйверів код.

Інтерфейс драйвера служби ***SPI*** *(Service Provider Interface)* – це інтерфейс між мережевими драйверами та MPR. Він дає змогу встановити багато мережевих драйверів та надає набір функцій для звертання до мережевих служб. MPR використовує функції SPI для звертання до мережевих драйверів (це функції верхнього рівня – розпізнавання користувача, приєднання до та від'єднання від мережевих ресурсів, керування паролями та ін.). Стандартизовані функції інтерфейсу драйвера служби дають змогу стороннім розробникам вводити у W95 свої мережеві служби.

Мережеві драйвери – це програми, орієнтовані на конкретний тип мережі. Вони повинні забезпечувати надання визначеного переліку служб у стандартизованому форматі. MPR передає виклики від API до мережевого драйвера з використанням інтерфейсу драйвера служби.

Диспетчер ***IFS*** *(Installable File System)* керує процесами передавання інформації від мережевих клієнтів. Фактично цей диспетчер є редиректором, який переспрямовує потоки введення-виведення з урахуванням різних файлових систем (VFAT, CDFS, FAT32) у мережу (файли vredir.vxd – мережі Microsoft, nwredir – мережі Novell). Можна додавати драйвери інших файлових систем інших виробників.

Мережеві клієнти у W95 реалізують головні файлові функції (шукання, читання, записування, знищення, створення файлів) з використанням відповідних файлових протоколів (SMB для мереж Microsoft, NCP для мереж Novell). W95 підтримує 32-розрядні клієнти захищеного режиму для мереж Microsoft та Novell, а також 16-розрядний клієнт реального режиму.

Сервери. Комп'ютер W95 може бути сконфігурований як мережевий сервер з виділенням ресурсів для спільного використання. W95 підтримує дві 32-розрядні серверні служби – доступ до файлів і принтерів мереж Microsoft та аналогічну службу для мереж Novell. Одночасно на комп'ютері може діяти тільки одна з цих служб. Служби дають змогу клієнтам відповідних ОС мати доступ до сервера W95.

Мережеві протоколи. W95 підтримує одночасно три різні транспортні протоколи: SPX/IPX, NETBEUI, TCP/IP. Мережеві протоколи реалізовані як 32-розрядні драйвери VXD:

• *SPX/IPX* реалізовано у файлах nwlink.vxd або nwnwnblink.vdx. Протокол підтримує 32-розрядні застосування Windows Sockets, а також автоматичне виявлення типу кадру Ethernet;

• *NETBEUI* реалізовано у файлі netbeui.vxd. Протокол сумісний зі стандартним протоколом NETBEUI мереж Microsoft, IBM;

• *TCP/IP* реалізовано у файлах vtcp.386 та vip.386. Протокол 32-розрядний, працює в захищеному режимі, підтримує протокол PPP, а також службу DHCP.

Драйвери мережевих адаптерів. W95 підтримує драйвери мережевих адаптерів у форматах NDIS 3.1, 2.x та ODI. NDIS 3.1 – це 32-розрядний драйвер захищеного режиму, що підтримує технологію Plug and Play. Його можна реалізувати в одному з двох варіантів: або у вигляді монолітного стандартного драйвера, або як сукупність двох компонент – програми-оболонки ndiswrap.vxd та програми мінідрайвера з розширенням sys, яку створює розробник адаптера. Остання конфігурація називається драйвером мініпорту.

34.3. Інсталювання та налагодження мережевих компонент

Мережеві компоненти можна інсталювати як під час інсталювання самої ОС, так і під час роботи системи. Розробники ОС намагалися максимально спростити процес інсталювання на окремій станції, приховати деякі його складні нюанси, зрештою автоматизувати процес інсталювання різних конфігурацій системи для великої кількості комп'ютерів. Ми звернемо увагу на головні принципи та підходи, технічні й системні вирішення, застосовані у процедурах інсталювання мережевих компонент W95. Детальна ж послідовність дій у цьому випадку описана в [1].

Перед інсталюванням W95 треба вибрати місце розташування системи (локальний ПК або сервер), місце, з якого виконувати інсталювання (локальний ПК або сервер), а також варіант початкового завантаження системи (з твердого диска локального ПК, сервера, гнучких дисків). Залежно від місця розташування системи розрізняють такі конфігурації:

• локальну; усі файли W95 розташовані на клієнті, інсталювання виконують з локальних дисководів або з сервера. Така конфігурація збільшує швидкодію роботи системи, однак потребує значного дискового простору;

• сумісного використання; частина файлів є на клієнті, головна – на сервері. Систему інсталюють з сервера. Це дає змогу зекономити ресурси, однак призводить до зменшення швидкодії роботи W95 порівняно з локальним інсталюванням.

Залежно від місця, з якого інсталюють систему, можливі такі варіанти:

• інсталювання з локального дисковода. У цьому випадку програма-дистрибутив міститься на локальному комп'ютері. Система розміщена у визначеному каталозі локального ПК (локальне інсталювання). Використовують для інсталювання окремих, необ'єднаних мережею станцій. Забезпечує менше можливостей для автоматизації процесу інсталювання.

• інсталювання з сервера. Програму-дистрибутив розміщують на сервері. Для такого типу інсталювання потрібне попереднє приєднання до сервера в уже наявній мережі. Допуска-

ється як локальне інсталювання, так і інсталювання сумісного використання. З сервера можна виконувати інсталювання на багато станцій одночасно, застосувати засоби автоматизованого інсталювання. У разі інсталювання з сервера програму-дистрибутив попередньо копіюють на диск сервера (команда netsetup).

Розглянемо детальніше процес інсталювання з погляду засобів його автоматизації.

Першим таким засобом треба вважати змогу **автоматичного розпізнавання типу адаптера та задання потрібних параметрів** (технологія *Plug and Play*). Задані параметри адаптера (номер переривання, адреса введення-виведення), які можна пізніше записати і вручну. Система буде фіксувати можливі конфлікти і підказувати діапазони можливих значень.

Другим засобом є **інсталювання мережевих компонент за замовчуванням**. Під час інсталювання користувач визначає потребу використання різноманітних мережевих компонент. *У разі вибору однієї компоненти автоматично інсталюються й інші, залежні від неї, у стандартних конфігураціях.* У цьому випадку користувач згодом зможе не тільки переглянути задану конфігурацію, а й модифікувати її згідно зі своїми потребами. Наприклад, якщо виявлено мережевий адаптер, то автоматично інсталюються такі компоненти:

• клієнт для мереж Microsoft. Дає змогу комп'ютеру стати клієнтом мереж SMB (Service Message Block – протокол передавання файлів) – WNT, Windows 3.11, LAN Manager, OS/2 LAN Server;

• клієнт для мереж Netware. Дає змогу комп'ютеру стати клієнтом мереж Netware 2.15–3.x. Версія 4.x працює тільки в режимі емуляції bindery;

• SPX/IPX сумісний протокол;

• NETBEUI.

Третім засобом автоматизації інсталювання треба вважати можливість створення та **використання текстових командних файлів** керування інсталюванням. Назву командного файлу (з розширенням inf) можна задати в командному рядку:

setup myfile.inf

Якщо назва файлу не зазначена, використовується системний файл msbatch.inf. Командний файл має власний формат. У цей файл можна записати такі параметри: передусім ті, які записує користувач вручну під час інсталювання, параметри вибирання й налагодження протоколів та інших мережевих компонент, список додаткових програм, які треба проінсталювати (в тому числі й ті, що не є у складі дистрибутива W95 – використання утиліти infinst). У командних файлах адміністратор може активізувати користувацькі профілі та ввімкнути підтримку системних правил.

Використання командного файлу дає змогу повністю автоматизувати процес інсталювання і виконувати його одночасно на великій кількості комп'ютерів без участі оператора. Для формування командного файлу можна використати програму batch.exe. Це компактна утиліта, за допомогою якої можна створити до 9999 пакетних файлів інсталювання (тобто за один раз інсталювати ОС на 10000 комп'ютерів). Ці файли розміщені в окремому каталозі (bstp00001.inf–bstp9999.inf).

Файли узагальнюють у провідному текстовому файлі, що складається з рядків

ім'я PC [, адреса IP]

Кожен рядок відповідає комп'ютеру, на якому відбувається інсталювання. Утиліта також дає змогу відкривати наявні командні файли та модифікувати їх. У процесі її роботи задають усі головні параметри інсталювання. Наприклад, можна примусити зберігати uninstall-інформацію, задавати набір необов'язкових компонент.

Автоматичне інсталювання можна виконувати такими шляхами:

• використати пакетний DOS-файл з командами налагодження мережевого сполучення та запуску інсталятора;

• застосувати макрос відкривання сеансу під час входження у мережу;

• використати групу автозапуску;

• можна відправити об'єкт електронної пошти, у разі вибору якого користувачем автоматично запуститься інсталятор;

• використати програмне забезпечення керування мережею, програми дистанційного керування.

34.4. Робота в мережі

Мережеві компоненти та їхнє налагодження. За структурою та інтерфейсом взаємодії з оператором W95 – це об'єктно-орієнтована ОС. Тому вона є набором компонент зі своїми властивостями. Одні й ті ж операції у W95 можна виконати кількома різними шляхами.

Після інсталювання системи користувач має деяку мережеву конфігурацію, параметри якої визначені у процесі інсталювання. Однак і під час роботи системи користувач має змогу аналізувати цю конфігурацію, інсталювати або деінсталювати її компоненти.

Розглянемо окремі мережеві компоненти детальніше.

Адаптери. W95 безпосередньо взаємодіє з відповідним драйвером адаптера, підтримує драйвери у форматах NDIS 3.1 (32-розрядний), NDIS 2.x (16-розрядний) та ODI. Не підтримується драйвер формату NDIS 3.0, що був у Windows 3.11.

Протоколи. Загальною ознакою форматів драйверів NDIS та ODI є забезпечення багатопротокольного стека. Кілька протоколів використовують для передавання один і той же адаптер. Кажуть, що протоколи закріплені за адаптером (прив'язані, bind). У W95 протоколи реалізовані як 32-розрядні драйвери захищеного режиму VXD (Virtual Device Drivers). Підтримуються такі протоколи:

• NETBEUI (NetBIOS Extended User Interface) сумісний зі стандартним протоколом NETBEUI, який використовують у Windows 3.11, Windows NT (WNT), OS/2, LAN Server; розроблений IBM; не підтримує передавання маршрутної інформації, однак може працювати з мостами;

• SPX/IPX;

• TCP/IP.

Клієнти. Клієнтський компонент забезпечує комп'ютеру доступ до серверів відповідних мереж. Для кожного типу мережі є окрема клієнтська компонента.

Клієнти бувають 32-розрядного захищеного та 16-розрядного реального режимів. Можна інсталювати один клієнт реального та довільну кількість клієнтів захищеного режиму. У дистрибутив W95 входять клієнти мереж Microsoft, Novell, FTP, Sunsoft, Banyan.

Клієнт для мереж Microsoft дає змогу працювати з усіма SMB-сумісними мережами, а клієнт для мереж Novell – з усіма NCP (Netware Core Protocol)-мережами. Сьогодні клієнт не підтримує NDS Novell 4.x, а працює з ним тільки в режимі емуляції bindery.

SMB та NCP – це протоколи сумісного використання файлів. Вони регулюють розподіл файлів між робочими станціями. Ці протоколи не обирають індивідуально, а вони вбудовані в клієнтські та сервісні компоненти ОС.

У W95 один протокол може бути прив'язаний до кількох клієнтів або кілька протоколів до одного клієнта (рис. 34.2).

Однак взаємодію сервер-клієнт реалізують одним протоколом.

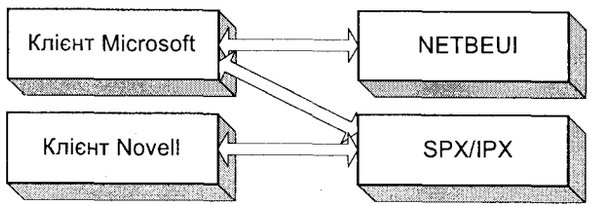


Рис. 34.2. Прив'язування протоколів до клієнтів.

Служби. Мережева служба – це сукупність засобів, які дають змогу вирішувати конкретну сервісну функцію (сумісне використання принтерів та файлів, підтримка створення мережевих резервних копій та ін.). У W95 є дві служби, що забезпечують клієнтам інших мереж доступ до файлових та принтерних ресурсів локального комп'ютера:

File and Printer Sharing for Microsoft Networks
File and Printer Sharing for Netware Networks

Ці служби інсталюються за замовчуванням.

Реєстрація користувача у системі. У W95 можна задати один з трьох варіантів реєстрації:

- *клієнт для мереж Microsoft.* Налаштовується за замовчуванням;
- *клієнт для мереж Netware*;
- *звичайне входження у Windows.* Не діє механізм захисту щодо користувачів – якщо під час першого запуску не зазначати пароль, то вікно ідентифікації користувача не з'являтиметься. Ім'я та пароль запитують тільки у випадку активізації користувацьких профілів.

Якщо визначено приєднання до мережі Microsoft, то введене ім'я та пароль перевіряються на сервері WNT.

Аналогічно, якщо приєднуватися до сервера Netware, W95 запам'ятовує паролі зі списку паролів і не запитує про них у разі наступних спроб приєднатися до мережевих ресурсів. Якщо пароль входження у W95 зробити порожнім і увійти в сервер WNT або Netware, то у випадку наступної спроби увійти в систему вона пароля не запитуватиме, і користувач зможе приєднатися до сервера без перевірки.

Якщо ваші ім'я та пароль входження у W95 збігаються з іменем та паролем входження у WNT або Netware, то ці дані є перепусткою на відповідний сервер. Якщо ж ім'я та пароль невідомі серверу, то у разі приєднання до нього треба ввести ім'я та пароль, які будуть збережені у списку паролів користувача. Наступного разу пароль читатиметься зі списку.

Використання засобу *Network Neighborhood (NN).* За допомогою NN можна виконувати значну кількість операцій. Наприклад, переглядати спільні ресурси на серверах мережі або відображати ресурс на мережевий диск. У цьому випадку первинним форматом відображення ресурсу є **UNC** (Universal Naming Convention)-нотація:

\\ім'я комп'ютера\ресурс.

У мережі W95 кожен комп'ютер має унікальне ім'я, визначене під час інсталювання системи. Ресурс може зображати диск комп'ютера, каталог або принтер. Використання UNC-формату дає змогу уникнути обмежень щодо кількості мережевих ресурсів. Відображення ресурсу на його позначення (наприклад, D:, G: або LPT1:) називається *перехопленням* (capture).

Під час перегляду мережевих ресурсів система використовує паролі зі списку або запитує їх.

Приєднання до мережевих принтерів. Перш ніж приєднуватися, треба інсталювати драйвер принтера. Це можна виконати з інсталяційного диска. Інсталюючи принтер у W95, ресурс можна задавати в UNC-нотації. Однак застосування DOS не розуміють UNC-формату, тому треба реалізовувати перехоплення принтера, що відбувається автоматично у разі вибирання опції роботи з DOS під час інсталювання принтера або через пункт меню *Призначити порт*.

Перегляд та приєднання/від'єднання мережевих дисків можна виконувати також засобами програми *Explorer*.

Робота з командним рядком. Командний рядок W95 дає змогу вводити глобальні для всієї системи команди, запускати windows-програми, а також цілі командні файли. Назвемо деякі команди:

net config	відображення поточної конфігурації PC;
net diag	запуск програми діагностування мережі. Перший PC з запущеною командою буде діагностичним сервером, надсилатиме за запитом інших станцій діагностичну інформацію;
net help	допомога;
net password	зміна пароля для відкривання сеансу на конкретному сервері або домені;

net print	відображення інформації про чергу для друкування і керування завданнями з друкування;
net time	синхронізація часу на локальному PC з годинником сервера;
net use	відображення наявних сполучень з мережевими дисками та принтерами, їхнє налагодження та переривання;
net ver	відображення номера версії програми;
net view	список серверів групи та їхніх ресурсів.

Якщо ім'я комп'ютера містить пропуск, то команда net з ним не працює.
Формат net use:

net use [пристрій:] \\комп'ютер\ресурс [пароль|?] [/savepw:no] [/yes] [/no]

savepw:no означає, що пароль не треба запам'ятовувати у списку паролів; [/yes] [/no] – визначення варіантів автоматичних відповідей на всі запитання. Для від'єднання використовують ключ /d.

34.5. Керування мережею

Ідентифікація комп'ютера та механізми обмеження доступу. Під час інсталювання визначають мережеве ім'я та групу, до якої належить комп'ютер. Однак ці параметри можна змінити. Робоча група – це лише зручний засіб для групування комп'ютерів.

У W95 визначено два механізми керування доступом до ресурсів. Керування доступом на рівні ресурсів дає змогу призначати паролі довільному ресурсу. Керуванням на рівні користувачів визначають конкретних користувачів або їхні групи, що мають доступ до кожного ресурсу. Керування доступом на рівні користувачів можливе тільки у разі приєднання до серверів Netware або WNT. У цьому випадку відповідні права читаються з цих серверів. Якщо доступ діє на рівні ресурсів, то W95 дає змогу задати повний доступ або доступ для читання, якщо ж на рівні користувачів, то, крім повного доступу та доступу за читанням, можна ще задати права на:

- записування файлів;
- створення файлів та папок;
- знищення файлів;
- зміну атрибутів файлу;
- друкування файлу;
- зміну керування доступом.

Незважаючи на те, що Netware та WNT дають змогу призначати права доступу до окремих файлів та каталогів, за допомогою W95 можна призначати права тільки для каталогів. За замовчуванням діє керування доступом на рівні ресурсів. Вибір типу сервера одержання інформації про права доступу користувачів визначається заданою службою взаємодії з конкретним типом мереж (Microsoft або Netware).

Спільне використання файлів та принтерів. Комп'ютер можна сконфігурувати як файловий сервер або сервер друкування. За замовчуванням сумісне використання не діє. Каталог сумісним можна зробити в *Explorer*, зазначивши мережеве ім'я ресурсу. Щоб інші користувачі не могли переглядати ім'я цього ресурсу, у кінець імені додають $, наприклад, *public$*. Задають тип доступу: тільки для читання, повний, визначений паролем.

Якщо визначений доступ на рівні користувачів, то задають також ім'я ресурсу. Крім того, виводиться список користувачів та груп, що мають право доступу до ресурсу. Якщо вводять нових користувачів, то можна задати тип доступу (читання, повний або спеціальний). Режим *спеціальний* дає змогу задати права доступу.

Сумісним використанням принтерів керують так само, як і сумісним використанням файлів.

Реєстр W95 та керування мережевими параметрами. Головними об'єктами керування є системний реєстр, користувацькі профілі, системні правила. Кожен користувач може мати власні налаштування (свій профіль). До профілю належать конфігурація робочого столу, зміст меню та ін. Користувач може мати доступ до свого профілю з довільного комп'ютера. Системний реєстр складається з двох файлів: user.dat (користувацькі налаштування, незалежні від комп'ютера, переміщуються з користувачем на інші ПК) та system.dat (системні та апаратні параметри, залежні від ПК, не переміщуються). Системні правила дають змогу адміністратору визначати права для користувачів та системні параметри для ПК.

Системний реєстр W95 – це ієрархічна база даних для збереження системної інформації; ini-файли використовують частково для застосувань, які не взаємодіють з реєстром. За замовчуванням системні файли містяться в каталозі \Windows\System, проте можуть бути і в інших каталогах.

Програма роботи з реєстром – regedit. Головні папки реєстру:

- HKEY_LOCAL_MACHINE,
- HKEY_USERS,

відповідають файлам реєстру. Інші папки є окремими гілками цих двох папок:

- HKEY_CURRENT_CONFIG відповідає розділу config HKEY_LOCAL_MACHINE;
- HKEY_DYN_DATA означає області, що містять інформацію про пристрої Plug and Play;
- HKEY_CLASSES_ROOT – це розділ HKEY_LOCAL_MACHINE\Software\Classes для асоціювання файлів з застосуваннями;
- HKEY_CURRENT_USER – це розділ HKEY_USERS, що містить інформацію про профіль користувача, який використовує ПК в конкретний момент.

Окремі розділи HKEY_LOCAL_MACHINE такі:

- Config – різні апаратні конфігурації, можливі для комп'ютера;
- Enum – інформація про пристрої комп'ютера. Монітори, НТМД, НГМД, мережеві протоколи та ін.;
- Network – інформація про конфігурацію мережі;
- Security – інформація про безпеку та дистанційне адміністрування;
- Software – програмне забезпечення, встановлене на комп'ютері;
- System – інформація про драйвери, служби, назву комп'ютера, параметри файлової системи та ін.

Окремі розділи HKEY_USERS:

- Control Panel – користувацьке налаштування панелі керування;
- InstallLocationMRU – список шляхів інсталювання W95 та інших продуктів;
- Network – список популярних мережевих сполучень;
- RunMRU – список застосувань, що їх використовують популярні мережеві сполучення;
- RemoteAccess – параметри віддаленого доступу;
- Software – програмні налаштування користувача для застосувань;
- StreamMRU – документи, які використовували останнім часом.

Імпортування та експортування даних з реєстру. Можна імпортувати окрему гілку реєстру (з усіма вкладеними) або весь реєстр. Експортований файл має текстовий формат, його можна змінювати текстовим редактором. Експорт та імпорт можна виконувати і з командного рядка.

Імпорт:

```
regedit [/I:system] [/r:user] filename.reg
```

Розміщення системних файлів

Назва файлу, який імпортують

Якщо імпортують частину файлу, то вона замінює відповідні розділи реєстру.

Експорт:

```
regedit [/I:system] [/r:user] /e filename.reg  [regkey]
```

Параметр regkey задає початковий ключ реєстру, з якого відбувається експорт. Якщо треба повністю замінити реєстр, використовують ключ /c.

Профілі користувачів. У них зберігається інформація про налаштування робочого столу, популярні мережеві ресурси, сполучення. Локальні профілі користувачів містяться у папці \Windows\Profiles. Кожен користувач має окрему папку, в якій є ще такі папки:

- Desctop – ярлики на робочому столі;
- NetHood – інформація про вікно мережевого оточення;
- Recent – вміст пункту *Документи* головного меню;
- Start Menu – зміст меню *Старт*;
- user.dat – користувацька частина системного реєстру;
- user.da0 – її копія.

Розташування каталогу, який містить файл зі списком шляхів відшукання профілів користувачів, визначене ключем

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\ProfileList
```

У разі входження користувача в систему введене ним ім'я є основою для шукання файлу користувацьких профілів. Паролі містяться в каталозі \Windows. Файл паролів zak.pwl.

Для того, щоб використовувалися профілі з локальної машини, а не з сервера, треба задати в розділі реєстру HKEY_LOCAL_MACHINE\Logon новий параметр *UseHomeDirectory* типу dword, який діє для конкретного комп'ютера і всіх користувачів, що працюють на ньому. Якщо користувача немає, використовується профіль за замовчуванням.

Профілі користувачів у мережевому середовищі можуть зберігатися на сервері. Під час входження користувача порівнюються профілі на сервері та локальний і вибирається найновіший. Після цього оновлюється серверний профіль. Цей профіль оновлюється і під час виходу користувача. Інформація про профілі може зберігатись на сервері WNT, Netware, W95. Загальні умови для роботи з серверним збереженням профілів користувачів такі:

- повинен бути відповідний 32-розрядний клієнт;
- мережевий сервер повинен підтримувати довгі імена файлів;
- на всіх клієнтах каталог W95 повинен мати однакову назву.

Умови роботи з сервером WNT. Користувач має базовий каталог на сервері. Активізовані профілі. Опція входження – приєднання до домену WNT (якщо вибрати швидке входження, то читання профілів з сервера не відбудеться, активізується локальний профіль і профілі оновляться за локальним (який може бути застарілим)).

Робота з W95-сервером. У HKEY_LOCAL_MACHINE\Network\Logon введено значення SharedProfileList та UseHomeDirectory. Перше означає файл зі списком профілів. Наприклад, це UNC – *.ini файл з такими рядками:

```
[Profiles]
Dana=\\zak\public\dana\user.dat
Katie=\\zak\public\katie\user.dat
```

В ОС W95 можливе застосування обов'язкових профілів користувачів, які зберігаються на сервері. Їх не може змінити користувач. Файл user.dat на сервері перейменовують на user.man.

Системні правила дають змогу гнучкіше адмініструвати роботу окремих користувачів та їхніх груп. Головні їхні функції та положення:

- системні правила можна використовувати окремо для користувацької та системної частин реєстру;
- можна застосовувати індивідуальні та групові правила з перекриттям;
- а також обов'язкові профілі та системні правила одночасно.

Умови використання системних правил такі:

- для реалізації користувацьких правил – активізовані профілі;
- на сервері WNT або Netware зберігається файл системних правил config.pol;
- якщо використовують інший сервер – це треба відобразити у реєстрі.

Для створення системних правил застосовують редактор poledit.exe, який комплектують файлом-шаблоном admin.adm, що визначає, які параметри системного реєстру доступні у редакторі. Файл-шаблон можна редагувати та додавати до нього нові параметри. Файл системних правил містить правила *Стандартний комп'ютер* та *Стандартний користувач*.

Кожен елемент у редакторі можна відмітити як реалізований, нереалізований, незмінний. Перші два змінюють відповідний параметр у системному реєстрі: реалізований – налагоджує, нереалізований – скидає. Незмінний залишає задане користувачем значення.

Схема застосування правил. Для кожного користувача передбачені конкретні правила, які починають діяти після відкриття сеансу. Якщо користувач не має персональних правил, однак входить у групи, то діють правила груп. Завантаження правил відбувається від найменшого пріоритету до найбільшого. Якщо для користувача нема жодних правил, діють правила *Стандартний користувач*. Правила застосування комп'ютерних правил аналогічні.

Окремо з диска налагоджують редактор системних та групових правил \admin\apptools\poledit. Групові правила діють на всіх ПК, де є групи. Редактор системних правил працює у двох режимах – файлу правил (зміна файлу правил) та реєстру (зміна параметрів реєстру з використанням шаблонів правил). Під час створення нового файлу правил автоматично створюються об'єкти *Стандартний користувач* та *Стандартний комп'ютер*. Нові правила є стандартними, потім їх змінюють вручну. За допомогою редактора правил можна модифікувати правила на віддаленому комп'ютері.

Розміщення config.pol:

WNT: \\server_name\netlogon\
Netware: \\server_name\sys\public\

Налаштування.

Користувацькі:

- панель керування: екран, мережа, паролі, принтери, система;
- робочий стіл: фон, кольорова схема;
- мережа: доступ;
- оболонка: власні папки, обмеження;
- система: обмеження.

Системні:

- мережа: керування доступом, вхід у мережу, клієнт Microsoft, клієнт Netware, сумісний доступ до файлів та принтерів, паролі, віддалений доступ до мережі, доступ, SNMP, оновлення;
- система: дозвіл на створення конфігурацій для користувачів, мережевий шлях для інсталювання Windows, мережевий шлях до підручника, завантажувати під час запуску, запускати служби.

Віддалене керування. W95 має засоби, що дають змогу виконувати віддалене керування комп'ютером з W95 з іншого комп'ютера. Головні функції віддаленого керування такі: перегляд та модифікація віддаленого системного реєстру; перегляд завантаження та поточної мережевої активності віддаленого комп'ютера з використанням *інспектора мережі*; перегляд параметрів роботи віддаленого комп'ютера з використанням системного монітора; доступ до диска віддаленого комп'ютера з використанням NN. Крім того, W95 має низку системних агентів, що пристосовані для виконання функцій керування, архівування.

Для роботи з віддаленим керуванням його треба активізувати на обох комп'ютерах. Дозвіл на керування одержують адміністратори мережі (якщо задано доступ на рівні користувачів, список адміністраторів керування можна змінити) або фіксується пароль доступу (якщо доступ задано на рівні ресурсів).

Віддалене керування ліпше виконувати з доступом на рівні користувачів. Якщо задано доступ на рівні ресурсів, деякі утиліти (редактор реєстру та системних правил, системний

монітор) будуть недоступні. На обох комп'ютерах повинен бути однаковий тип доступу до ресурсів. Під час налагодження віддаленого керування створюють два спільні каталоги: admin$, ipc$. Перший з них надає доступ до файлової системи на віддаленому комп'ютері, другий забезпечує зв'язок між процесами на двох комп'ютерах.

Інсталювання та робота з віддаленим реєстром. Віддалений реєстр – це окрема служба, яку запускають так: d:\admin\nettools\remotreg.

Він працює тільки в мережах з серверами NT або Netware.

Після налагодження служби редагування реєстру операції редагування можна виконувати засобами редактора системного реєстру та в редакторі системних правил.

Використання 'інспектора мережі'. Утиліта *Netwatch* дає змогу керувати використанням віддалених комп'ютерів, бачити хто працює з віддаленим комп'ютером, скільки відкритих файлів у сеансі. На ПК повинна бути служба доступу до файлів. Адміністратор може від'єднувати користувача від віддаленого комп'ютера, створювати та знищувати каталоги спільного використання, переглядати список та закривати відкриті файли.

Використання системного монітора. Діє віддалене керування та служба 'віддалений реєстр'. Використовується стандартна програма sysmon з усіма її можливостями.

У W95 реалізовані такі *агенти*:

- агент мережевого монітора Microsoft. Працює як служба. Передає всю інфомацію про роботу системи у програму *Network monitor (WNT)*. Використовується програма netmon;
- агент Microsoft SNMP. Дає змогу використовувати засоби керування третіх фірм;
- агенти одержання резервних копій.

34.6. Електронна пошта. Microsoft Exchange та Microsoft Fax

У W95 можна виділити таку ієрархію поштових служб:

- для організації електронної пошти у межах локальної мережі використовують службу Microsoft Mail;
- для роботи пошти у конфігурації кількох локальних мереж з серверами WNT потрібно встановити на сервері WNT продукт Microsoft Mail Server;
- для виходу в глобальні мережі можна використати ПЗ приєднання до **MSN** (Microsoft Network) або безпосередньо до Internet.

Універсальним клієнтом електронної пошти є *Microsoft Exchange (**ME**)*. Він дає змогу приєднатись до Compuserve, Microsoft Mail, Internet Mail, MSN. ME реалізований як служба. Крім ME, є аналогічна служба Microsoft Fax.

Створення поштового відділення Microsoft Mail. Для роботи електронної пошти Microsoft Mail треба створити поштове відділення (центральне сховище пошти).

Спочатку інсталюють Microsoft Exchange без адреси поштового відділення. Формується папка Inbox. Вибирають *ручне налагодження служб*; ім'я конфігурації вибирають *за замовчуванням*. На панелі керування з'являються дві піктограми – Mail and fax, Microsoft Mail Postoffice.

Розглянемо процес створення поштового відділення. Спочатку визначають місце розташування поштового відділення – наявний каталог або диск. За визначеною адресою створюють поштове відділення у вигляді папки wgpo0000, що міститиме свої каталоги. Вводять інформацію про адміністратора (ім'я, поштова скринька, пароль). Адміністратор зможе залучати нових користувачів та виконувати інші адміністративні функції. Перед початком роботи пошти каталог поштового відділення треба визначити як спільний ресурс повного використання.

Після цього для кожного, хто планує користуватись поштою, треба створити обліковий файл.

Наступним етапом є створення служби Microsoft Mail. Спочатку створюють Microsoft Exchange, проте задають опцію *вибрати інформаційні служби* та адресу поштового відділення. Вибирають ім'я зі списку зареєстрованих у поштовому відділенні та пароль. Після цього поштова служба користувача вважається створеною (іншого користувача можна ввести через відповідні профілі).

Використання Microsoft Exchange. ME запускають піктограмою Inbox. У цьому випадку запитується пароль доступу до поштового відділення. Якщо користувач працює з різними комп'ютерами, то пошта кожного сеансу пересилається на ПК, з якого увійшов користувач. Після переміщення користувача на новий ПК стара пошта не знищується, однак до неї мають доступ інші користувачі. Вирішити цю проблему можна, задавши свою персональну папку (Personal Folder) на сервері.

Після відкриття ME виводиться список нових листів. Пункти меню ME такі:

• *файл* – копіювання та переміщення повідомлень між папками. Перегляд файлових характеристик повідомлення. Імпорт особистих поштових та адресних книг;

• *редагування* вибраних елементів списку як прочитаних або непрочитаних;

• *перегляд* – створення нових форм екрана. Перегляд усіх папок, вхідних, вихідних, відправлених та знищених документів;

• *сервіс* – модифікування та конфігурування функцій ME. Вибирання поштової служби (Microsoft Mail, Microsoft Fax), робота з адресними книгами;

• *повідомлення*. Команди щодо роботи з новим повідомленням, його створення та пересилання.

Щоб стежити за читанням повідомлення з поштового сервера, використовують лічильник, значення якого зменшується на одиницю у випадку, коли повідомлення читає наступний користувач. Якщо лічильник містить 0, то повідомлення знищується.

Налаштування служби Microsoft Fax. Microsoft Fax (MF) дає змогу відправляти факси з комп'ютера, а також сумісно користуватися факсом. Факс-модеми можна застосовувати для відправляння та приймання файлів з використанням технології **BFT** (Binary File Transfer), яка є в W95, Windows 3.11 та інших системах, що підтримують стандарт Microsoft At Work. MF є продуктом у складі W95.

У W95 передбачено, що під час створення ME можна налагоджувати тільки MF або тільки Microsoft Mail. У цьому випадку Microsoft Fax вибирають як інформаційну службу пізніше. Факс-модем визначають з наявного списку. Через опцію *додати* можна вибрати або інший модем, або модем спільного використання на іншому ПК (мережевий факс-сервер). У разі звертання до мережевого факс-сервера треба задати UNC-адресу спільного каталогу факсу. Крім того, модем потрібно визначити як спільний, зазначивши ім'я користувача, код країни, номер факсу.

Властивості MF.

• *Повідомлення*. Час відправлення (якнайшвидше, у конкретний час, за пільговим тарифом). Формат повідомлення (з можливістю редагувати чи ні). Титульна сторінка.

• *Набирання номера*. Кількість повторень набирання та інтервал між ними. Властивості сполучення.

• *Модем*. Вибирання модема та задання режиму спільного використання. Встановлення кількох факс-модемів та вибирання активного. Режими набирання номера та відповіді.

• *Користувач*. Інформація, що буде з'являтися на титульній сторінці факсу.

Використання Microsoft Fax. Якщо є служба MF, то в ME можна скласти повідомлення і передати його на адресу, що містить номер факсу. У цьому випадку можна приєднувати файли, передавати їх у форматі, що дає змогу їх редагувати, використовувати факс-сервери. Задавши номер, можна змінити параметри модема. Якщо файл надсилають не в форматі редагування, треба вказати його розширення.

Використання особистої адресної книги. Створивши особисту адресну книгу, в неї можна копіювати фрагменти з загальної поштової книги, а також утворювати свої записи. Кілька користувачів можуть створити спільну адресну книгу. Кожен користувач може створити довільну кількість списків розсилання.

Використання Microsoft Network (MSN). *MSN – це оперативна служба Microsoft. Вона* надає послуги електронної пошти, приєднання до Internet та використання WWW.

Через MSN можна одержати доступ до Internet. Мережа MSN у цьому випадку є провайдером послуг Internet. Під час налаштування MSN можна вибрати одну з трьох служб:

• Microsoft Network;

• Internet and Microsoft Network;

• ISDN access to the Internet and MSN.

Тип служби визначає виняткове використання MSN або можливість виходу в Internet.

34.7. Віддалений доступ

W95 - це ОС, спеціально спроектована з функцією віддаленого доступу. Вона дає змогу мобільним користувачам приєднуватись як вузол мережі в будь-який час. Невелика перепускна здатність каналів зв'язку змушує пересилати файлову інформацію на віддалений комп'ютер (не завжди можна працювати в оперативному режимі).

Термінологія: комп'ютер, який викликають, називається віддаленим сервером (dial-up server), а комп'ютер, що викликає, – віддаленим клієнтом. Віддалений сервер W95 працює одночасно тільки з одним віддаленим клієнтом, WNT – до 256 клієнтів. W95 підтримує декілька типів сполучень: PPP та SLIP використовують клієнти W95, WNT 3.5, 4, RAS – клієнти Win-

dows 3.11, WNT 3.1. PPP забезпечує багатопротокольний зв'язок, RAS підтримує протоколи NETBEUI, SLIP – TCP/IP, NRN (Novell Netware Connect) – SPX/IPX.

Налагодження віддаленого доступу. Клієнта віддаленого доступу визначають під час інсталювання W95. Сервер налаштовують у MPlus! Якщо віддалений доступ налагоджено, то у вікні MyComputer є папка *Віддалений доступ*. Компонента віддаленого доступу має тип мережевого адаптера. Це означає, що мережеві протоколи автоматично прив'язані до адаптера віддаленого доступу.

Робота з віддаленим доступом. Папка віддаленого доступу зберігає задані сполучення та має об'єкт *нове сполучення*, вибравши який, можна створити нове сполучення, задавши модем, номер віддаленого сервера, ім'я сполучення. Властивості створеного сполучення можна змінити, у тому числі вибрати протокол доступу. За замовчуванням налаштовується PPP. Протокол SLIP приєднується через Windows Setup (→ have Disk → \admin\apptools\dscript\rnaplus.inf). W95 відрізняє мережеве сполучення та сполучення віддаленого доступу, використовує спеціальні засоби для збільшення перепускної здатності сполучення віддаленого доступу.

Налагодження сервера віддаленого доступу. Використовують папку *Віддалений доступ – Сполучення – Сервер віддаленого доступу*. Вигляд вікна конфігурації залежить від заданого режиму доступу (щодо ресурсів або користувачів). Забороняється (за замовчуванням) або дозволяється віддалений доступ, завдається пароль доступу до ресурсів або списку користувачів, що мають право доступу, вибирається тип сервера та протоколів.

Робота з віддаленим доступом через ME. ME аналізує наявність сполучення та його тип. Якщо сполучення немає, то можна вибрати один з трьох варіантів:

- задати сервер пошти в локальній мережі;
- використати віддалений доступ для налагодження з поштовим сервером; реально сполучення буде тільки у разі спроби передати дані;
- не налагоджувати сполучення з поштовим сервером; повідомлення зберігаються у черзі і в разі сполучення з сервером відразу передаються.

Пряме сполучення. Два ПК сполучають через послідовний або паралельний порти. Один з ПК стає головним (host), інший – приєднаним (guest). Приєднаний комп'ютер має доступ до ресурсів головного ПК і через нього вихід у локальну мережу (головний ПК діє як шлюз у мережу тільки для мереж SPX/IPX та NETBEUI, але не TCP/IP). Пряме сполучення налагоджують через Windows Setup: задають статус ПК, можливості парольного захисту та пароль.

Синхронізація файлів з використанням утиліти *Портфель*. Портфель – це особливий тип папки, який дає змогу стежити за станом скопійованих у неї файлів та папок. Портфелів може бути багато, їх переміщують на інші ПК та дискети. Щоб простежити статус файлу, його треба скопіювати, а не перемістити у портфель. Файл у портфелі може мати статус синхронізованого та 'сироти'. Для будь-якого синхронізованого файлу можна розірвати зв'язок з оригіналом. Синхронізація файлів відбувається під контролем користувача.

Дистанційне керування. W95 безпосередньо дистанційного керування не підтримує. Для цього можна використати продукти третіх фірм (pcAnywhere, Reachout). Дистанційне керування працює з більшою швидкістю, однак потребує окремого ПК в мережі.

34.8. Мережеві функції Windows 98

У 1998 р. фірма Microsoft випустила нову поліпшену версію ОС для настільних ПК – Windows 98 (W98). Особливості цієї ОС такі:

- W98 – це web-орієнтована ОС. Важливим її компонентом є браузер *Internet Explorer 4*, який забезпечує доступ до Internet. Web-інтерфейсу дотримуються й у випадку реалізації локальних операцій (роботи з папками, вікнами);
- реалізована концепція активного робочого столу, фоном якого може стати web-документ, який динамічно завантажується з каналів Internet;
- компонентами системи стали редактор web-документів *Frontpage Express*, програмне забезпечення web-сервера *Personal Web Server*;
- автори W98 відмовилися від концепції 'універсальної поштової скриньки', реалізованої у W95. Замість ME поштовим клієнтом є програма *Outlook Express*, яка функціонально відповідає ME. Крім роботи з поштою, вона дає змогу працювати з групами новин. Реалізована програма телеконференцій *Netmeeting*. Однак служба MF не підтримується;
- W98 підтримує службу каталогів NDS фірми Novell;
- реалізований новий формат драйверів пристроїв, який збігається з форматом драйверів WNT 4;
- віддалений доступ підтримує новий протокол ***PPTP*** *(Point-to-Point Tunneling Protocol)*, який забезпечує ліпший захист інформації під час передавання;
- підтримується архітектура розподілених обчислень DCOM, взаємодія компонент ActiveX, сценаріїв та аплетів Java для intranet та Internet;
- реалізовано компоненту *Windows update manager*, яка підтримує зв'язок з сервером Microsoft і періодично приймає інформацію про поновлення, виправлення помилок. Якщо виник збій, то *Windows report tool* зробить 'знімок' поточного стану системи і передасть його у службу підтримки користувачів Microsoft;
- утиліта *Sytem File Checker* відшукує змінені, зіпсовані або знищені системні файли і, якщо потрібно поновлює їх з дистрибутива;
- утиліта *Maintenance Wizard* дає змогу створювати розклад виконання періодичних операцій (наприклад, архівування даних) та виконувати їх.

Бібліографія та джерела

1. *Богумирский Б.* Энциклопедия Windows 98. СпБ: Питер, 1998.
2. *Мак-Федриз П.* Microsoft Windows 98. Энциклопедия пользователя. К.: Диасофт, 1998.
3. *Питрек М.* Внутренний мир Windows. К.: Диасофт, 1995.
4. *Штольц К.* Секреты сетей под Windows 95. К.: Диалектика, 1996.

МЕРЕЖЕВІ МОЖЛИВОСТІ WINDOWS NT

Загальна характеристика операційної системи Windows NT. Архітектура ОС. Архітектура мережевих засобів та системи безпеки. Загальна характеристика та головні принципи реалізації. Процес реєстрації у системі. Контроль доступу. Робочі групи та домени.

35.1. Загальна характеристика операційної системи Windows NT

Windows NT (Windows New Technology (WNT)) – це 32-розрядна операційна система з пріоритетною багатозадачністю. Вона належить до ОС, які працюють у режимі витіснення, з вбудованими мережевими функціями та системою безпеки. Інші характеристики цієї ОС такі:

- наявність графічного інтерфейсу;
- сумісність з різними ОС (OS/2, MS-DOS, Windows 3.x, 95, POSIX);
- можливість перенесення ОС на RISC- та CISC-процесори;
- масштабованість – можна працювати на одно- та багатопроцесорних системах, підтримка кластерів комп'ютерів;
- система безпеки створює для кожного застосування повністю незалежне оточення;
- поліпшені можливості локалізації завдяки підтримці стандарту ISO Unicode.

ОС Windows NT буває двох конфігурацій:

- **Windows NT Workstation** (робоча станція Windows NT);
- **Windows NT Server** (сервер Windows NT).

Windows NT Workstation підтримує роботу до десяти користувачів. Вона може виконувати серверні функції у невеликих мережах робочих груп. Windows NT Server орієнтовано на виконання серверних функцій у великих мережах з інтенсивним трафіком.

ОС WNT має модульну структуру. Головні вирішення, вперше застосовані у ній, були свого часу новаторськими. Багато з них запозичили інші операційні системи, зокрема Windows 95. ОС Windows NT не можна однозначно віднести ні до однорангових, ні до мереж з призначеним сервером. З одного боку, Windows NT підтримує однорангову модель, і навіть сервер Windows NT не є призначеним (за ним може працювати користувач). З іншого, у мережі WNT можна функціонально закріплювати за серверами та робочими станціями певні функції, конфігуруючи їх як файлові сервери, сервери баз даних, застосувань тощо. Така модель є гнучкішою, ніж у системах Netware. Цим пояснюється популярність WNT як ОС для систем керування нижчого та середнього класу складності.

35.2. Архітектура Windows NT

Для того, щоб ліпше зрозуміти мережеві функції WNT, розглянемо її архітектуру (рис. 35.1).

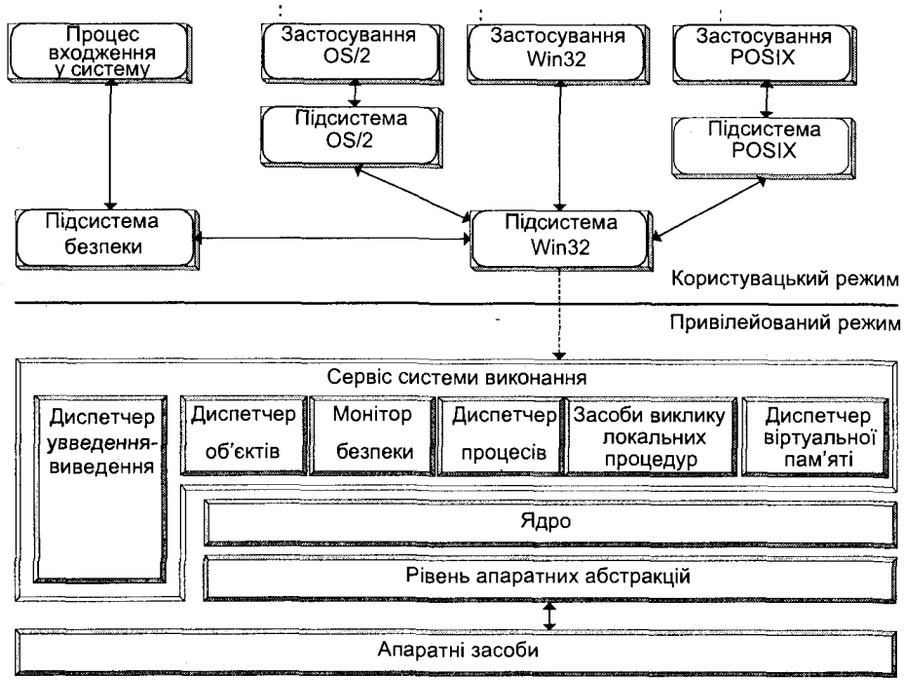


Рис. 35.1. Архітектура ОС Windows NT.

Рівень апаратних абстракцій (Hardware Abstraction Layer (HAL)) віртуалізує апаратні інтерфейси, робить решту операційної системи незалежною від конкретних особливостей апаратури. Цей рівень допомагає також переносити WNT на іншу апаратну платформу (ідею віртуалізації ми вперше описали на прикладі віртуального термінала, файлу, емуляції систем). Рівень апаратних абстракцій дає змогу 'приховати' від інших рівнів ОС особливості реалізації симетричних багатопроцесорних систем.

Ядро (Kernel) координує виконання базових операцій WNT. Воно відповідає за планування та диспетчеризацію роботи процесора(рів), зокрема диспетчеризацію різних потоків керування. Потік керування визначають у контексті процесу і він є деякою послідовністю команд. Процес у WNT може мати декілька таких потоків, виконання яких відбувається на кількох процесорах. Ядро виконує диспетчеризацію так, щоб найефективніше завантажити наявні про-

цесори та забезпечити пріоритетність опрацювання (визначено 32 рівні пріоритетів, структурованих у два класи: реального часу (real time) та змінний (variable)). Ядро керує двома типами об'єктів.

• **Об'єкти диспетчеризації** використовують для синхронізації системних операцій. Кожен з них має певний сигнальний стан. Об'єктами диспетчеризації є події, мутанти, мутекси, семафори, потоки керування та таймери.

• **Об'єкти керування** застосовують для реалізації функцій керування, однак безпосередньо вони на диспетчеризацію не впливають. До об'єктів керування належать асинхронні виклики процедур, переривання, процеси та профілі.

Ядро спеціально оптимізоване щодо розміру та ефективності функціонування. Воно постійно міститься у пам'яті.

Система виконання (executive) складається з окремих модулів, кожен з яких спроектовано для виконання визначеного набору функцій. Стосовно верхніх рівнів ієрархії у структурі ОС модулі працюють як сервери, за відповідними запитами надаючи сервісне обслуговування. Завдяки цьому досягається можлива оптимізація серверів на виконання своїх функцій, незалежність серверів та їхніх клієнтів, приховування деталей реалізації серверів від клієнтів, єдині інтерфейси запиту сервісів. Розглянемо функції окремих модулів.

Диспетчер об'єктів створює, знищує та стежить за використанням об'єктів процесами системи. До об'єктів належать деякі елементи ОС часу виконання, такі як об'єкти каталогу, об'єкти символьних зв'язків, семафори, події, процеси, потоки керування, порти, файли та ін. Після створення об'єкта диспетчер видає його вказівник та дескриптор. Отже, у структурі WNT значною мірою використана об'єктна парадигма.

Диспетчер процесів простежує об'єкти процесів та потоків керування. Для процесу визначають адресний простір, набір доступних об'єктів, сукупність потоків керування. Кожен потік керування має власний набір регістрів, стек ядра, блок середовища, стек користувача. Диспетчер процесів створює та закінчує процеси, однак не групує їх та не створює між ними відношень породження.

Диспетчер віртуальної пам'яті виконує сторінковий обмін процесів. Кожен процес може використовувати до 4 Гб власної віртуальної пам'яті, половина з якої відведена для системи, а решта – для програми. Диспетчер віртуальної пам'яті відображає віртуальні адреси в адресному просторі процесу на фізичні сторінки у пам'яті комп'ютера, реалізує режим незалежності адресних просторів різних процесів, через що один процес не може змінювати пам'ять іншого без дозволу.

Засоби виклику локальних процедур. Застосування та підсистеми середовища взаємодіють як клієнти з серверами. Для реалізації такого механізму WNT надає засоби виклику локальних процедур (Local Procedure Call (LPC)), що функціонують подібно до виклику віддалених процедур (RPC), однак оптимізовані для виконання на локальній машині. Ідеологія виклику повністю відповідає архітектурі DCOM (див. розділ 25). Взаємодія відбувається за допомогою передавання повідомлень. Процес проходження повідомлень прихований спеціальними затичками (stubs), які приймають запит від застосування, запаковують відповідні параметри та передають їх відповідній серверній підсистемі.

Диспетчер уведення-виведення. Головне призначення цього диспетчера – координування та керування роботою драйверів. WNT використовує драйвери пристроїв, файлової системи, мережеві. Диспетчер реалізує їхню взаємодію. Кожен з типів драйверів відповідає за логічно завершений набір функцій. Драйвери нижнього рівня керують фізичними пристроями комп'ютера. Драйвери верхніх рівнів не вникають у деталі реалізації та роботи пристроїв, а просто звертаються до драйверів пристроїв згідно з визначеними інтерфейсами. До драйверів верхніх рівнів належать **мережеві драйвери, файлові системи, мережеві редиректори.**

Драйвери взаємодіють між собою, надсилаючи спеціальні пакети введення-виведення диспетчеру введення-виведення, який або блокує виконання застосування до завершення виведення (синхронне введення-виведення), або дає змогу продовжити роботу відразу ж після розміщення запиту на виведення у черзі (асинхронне введення-виведення). Після завершення асинхронної операції диспетчер сигналізує застосуванню.

Серед драйверів виділяється єдиний **диспетчер кешу**, функцією якого є ефективне керування кешом – завантаження та вивантаження інформації з кешу для всіх файлових систем та мережевих застосувань, динамічне вибирання розміру кешу залежно від ємності вільної пам'яті, підтримка служб відкладеного фіксування та відкладеного записування (записування інформації або фіксування транзакційних змін у реєстрах відбуваються після того, як зменшиться завантаження процесора). WNT підтримує також кілька драйверів файлових систем (FAT, HPFS, NTFS).

Підсистеми середовища працюють у користувацькому режимі. Вони відображають верхній щодо системи виконання рівень абстракції. Головне завдання підсистем середовища – емулювати для застосування роботу у певній операційній системі. Вони є незалежними, захищеними процесами. Збій в окремій підсистемі не зумовить збою інших підсистем або ОС (за винятком центральної підсистеми Win32, збій у якій спричинює зависання системи).

35.3. Мережева архітектура Windows NT

Архітектура мережевих засобів WNT відповідає еталонній моделі взаємодії відкритих систем. Її можна розділити на рівні (рис. 35.2).

На нижньому рівні мережевої архітектури розташовані драйвери адаптерів. Це фрагменти коду, що сполучають WNT з мережею через мережеві адаптери. Драйвери адаптерів постачають їхні виробники. Вони взаємодіють з верхніми рівнями, дотримуючись вимог інтерфейсу NDIS.

Інтерфейс NDIS – це стандартизована специфікація (див. розділ 5), яка дає змогу через один адаптер передавати пакети кількох транспортних протоколів. Розробка цього інтерфейсу, як і інтерфейсу TDI, що є вище, була зумовлена потребами дотримання вимог еталонної моделі, забезпечення незалежності рівнів, стандартизації їхньої взаємодії.

Транспортні протоколи реалізовані у вигляді окремих драйверів пристроїв. Вони взаємодіють з адаптером через NDIS-сумісні дравери пристроїв. У складі WNT є такі транспортні протоколи:

• NBT – транспортний протокол, створений на базі немаршрутизованого протоколу NETBIOS;

• TCP/IP – протокольний стек (див. розділ13);

• NWlink – NDIS-сумісна версія протоколу SPX/IPX мереж Novell Netware;

• Appletalk – підтримує сервіси Macintosh на WNT.

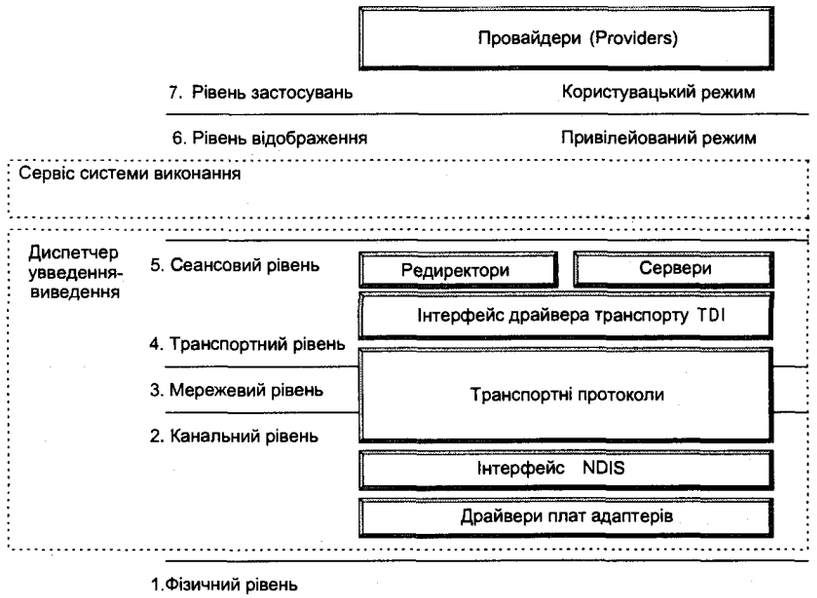


Рис. 35.2. Мережева архітектура Windows NT.

Над транспортними протоколами є інтерфейс драйвера транспорту (Transport Driver Interface (TDI)). Він визначає стандартний механізм доступу до функцій транспортного рівня для таких сеансових компонент, як редиректори та сервери. Отже, він виконує аналогічні до NDIS функції. TDI не є окремою програмною компонентою, а тільки специфікацією, згідно з якою створені транспортні драйвери.

Сеансовий рівень у мережевій моделі WNT репрезентують редиректори та сервери. Вони виконані у вигляді драйверів файлової системи. Такий підхід дає змогу використовувати однакові функції користувацького API для звертання до локальних та мережевих дисків. **Редиректор** разом з диспетчером уведення-виведення бере участь у переспрямуванні звертання до ресурсу. У разі доступу до ресурсу процес безпосередньо звертається до диспетчера введення-виведення, який визначає, чи ресурс міститься у мережі, та передає запит редиректору. Редиректор надсилає запит мережевим драйверам нижнього рівня. У WNT може працювати кілька редиректорів, по одному для взаємодії з кожним типом мереж. Функцією редиректора також є поновлення мережевого сполучення у разі його розірвання. **Сервер WNT** – це програмна компонента, завданням якої є обслуговування запитів. Вона підтримує сполучення, що їх запитує редиректор

клієнта, та забезпечує доступ до ресурсів. Драйвер сервера взаємодіє з драйвером локальної файлової системи.

Вище від рівня редиректорів, які працюють у привілейованому режимі, розміщена структура провайдерів (див. рис. 35.2). Провайдери використовують для взаємодії процесів застосувань з мережею. Вони співпрацюють з редиректорами. WNT має вбудований провайдер для зв'язку з іншими системами WNT. Провайдери інших систем можна інсталювати окремо. Головне призначення провайдерів – допомога у шуканні файлів за їхніми позначеннями. Структура провайдерів має дві додаткові компоненти, які спрямовують запити відповідному провайдеру:

• провайдер множинних UNC (Multiple UNC Provider (MUP));

• маршрутизатор множинних провайдерів (MPR).

Провайдер множинних UNC одержує назву ресурсу у форматі UNC:

\\server\share\subdirectory\filename.

Це компонента, що виконується у привілейованому режимі. Коли застосування звертається до ресурсу з іменем UNC, MUP звертається до всіх зареєстрованих провайдерів. Якщо провайдер підтверджує, що він може налагодити сполучення з відповідним ресурсом, то MUP надсилає йому весь запит.

Маршрутизатор множинних провайдерів виконує команди формату Wnet, який є складовою частиною інтерфейсу Win32 API, і подає різноманітні файлові системи в єдиному форматі.

35.4. Архітектура системи безпеки WNT

Система безпеки WNT сертифікована за рівнем С2. Головні її характеристики такі:

• власник ресурсу має змогу керувати доступом до нього;

• ОС захищає об'єкти від несанкціонованого доступу. Після вивільнення пам'яті або знищення файлу інформація стає недоступною;

• користувач, входячи у систему, вводить унікальні ім'я та пароль; ця інформація є перепусткою для всіх його подальших дій і всіх дій його процесів;

• адміністратор системи має змогу контролювати всі події, пов'язані з безпекою;

• система захищає себе від модифікації системних файлів та системної інформації на стадії виконання.

Систему безпеки можна вивчати як на рівні окремої станції, так і на рівні мережі WNT. У її основі є локальна система безпеки. Розглянемо її структуру (рис. 35.3).

Загальна характеристика локальної системи безпеки. Головні компоненти локальної системи безпеки такі:

• **процеси входження у систему**. Приймають запити користувачів на входження у систему та ініціюють перевіряння повноважень користувача. Процеси входження опрацьовують запити локального або віддаленого користувача;

• **розпорядник локальної безпеки**. Це головна компонента керування системи безпеки. Вона розпізнає користувача, створює для нього маркери доступу, керує політикою контролю та реєструє котрольні повідомлення монітора безпеки у спеціальному журналі;

• **диспетчер бюджету безпеки** підтримує базу даних бюджетів користувачів та груп, взаємодіє з розпорядником локальної безпеки;

• **монітор безпеки**. На відміну від попередніх компонент він працює у привілейованому режимі, перевіряє правомірність звертання процесу до ресурсу кожного разу під час спроби звертання і дає або не дає дозвіл. Отже, монітор безпеки реалізує політику безпеки на нижньому рівні.

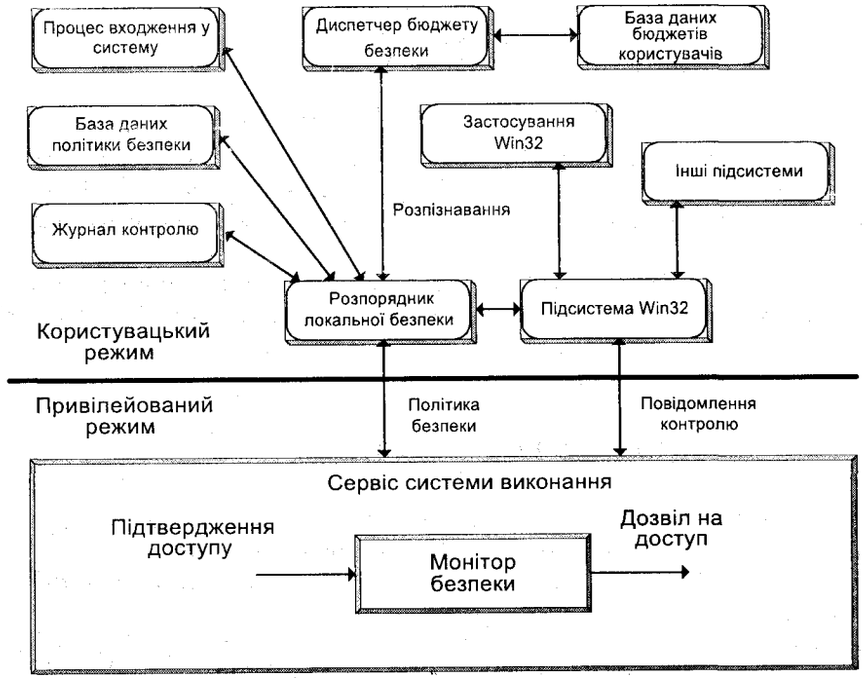


Рис. 35.3. Структура локальної системи безпеки.

Головні принципи організації локальної системи безпеки. Призначенням системи безпеки WNT є контроль за доступом до ресурсів системи. У системі, в спеціальній базі даних, зберігається інформація про користувачів, їхні групи, ресурси та права доступу. Процеси, що виконуються у WNT, асоціюються з певним користувачем, який їх запустив (діють від його імені).

Аналогічно до інших систем безпеки адміністратор може задавати права доступу до ресурсів. Перелік прав залежить від типу ресурсу. Наприклад, для файлу можуть бути такі права:

• читання (read);

• знищення (delete);
• записування (write);
• змінювання прав (change permission);
• виконання (executive);
• монопольне використання (take ownership);
• відсутність доступу (no access).

Як бачимо з переліку, ці права суттєво відрізняються від прав ОС Windows 95. Особливе значення мають права монопольного використання та явного задання відсутності доступу, вони ліпше захищають ОС.

Крім звичайних прав доступу до ресурсів, у WNT передбачені права на виконання певних системних дій (архівування, зміна системного часу, запуск системи та ін.).

Кожного користувача та групу ідентифікують за допомогою унікального *ідентифікатора безпеки (Security ID (SID))*. Коли користувач входить у систему, створюється *маркер доступу*. У нього записують ім'я та SID користувача, перелік назв груп, до яких він належить, та їхні SID. Після цього кожен процес, що виконується у системі від імені користувача, має копію маркера доступу. Інформацію з нього використовують для перевірки прав доступу процесу до ресурсу. Такий процес називається *суб'єктом* користувача. Кажуть, що він діє в контексті безпеки цього користувача. Це означає, що суб'єкт має права доступу до ресурсів, визначені правами цього користувача.

Деякі серверні процеси WNT можуть діяти від імені конкретного користувача. У цьому випадку вони тимчасово позичають атрибути його безпеки. Така техніка називається *перевтіленням (impersonation)*. Наприклад, коли сервер звертається до ресурсу на вимогу процесу-суб'єкта користувача, відбувається перевтілення і права доступу тимчасово переходять до серверного процесу.

Процес входження користувача у систему. Користувач, розпочинаючи роботу у системі, входить у неї за допомогою набору клавіш Ctrl-Alt-Del. Ця комбінація захищає процес розпізнавання від програм, що імітують процес входження користувача з метою зафіксувати його ім'я та пароль. Потім користувач уводить своє ім'я та пароль. Ці дані надходять у пакет розпізнавання, який перевіряє базу даних бюджетів. Якщо бюджет є локальним (тобто міститься у локальній базі), то порівнюються імена та паролі, якщо ж його не виявлено у базі, то пакет розпізнавання може або викликати інший, альтернативний розпізнавальний пакет, або видати помилку.

Після підтвердження достовірності користувача *Диспетчер бюджету безпеки* повертає пакетові SID користувача та всіх його груп. Ця інформація потрапляє до локального розпорядника безпеки, який і створює маркер доступу. Сеанс входження у систему, створений попередньо пакетом розпізнавання, викликає підсистему Win32, яка формує процес-суб'єкт для користувача з приєднаним маркером доступу.

Права доступу до об'єктів. Об'єктам ОС WNT можна призначити права доступу. Кожен об'єкт має спеціальний дескриптор безпеки – базу даних з такими структурними елементами:

• ідентифікатор безпеки власника (користувач або група);

• контрольований список керування доступом **ACL** (Access Control List), що ідентифікує об'єкти та права доступу їх до конкретного об'єкта;

• системний ACL, що керує переліком контрольних подій та повідомлень, які генерує система.

Серед об'єктів виділяють контейнерні (можуть містити інші об'єкти) та неконтейнерні. Якщо якісь права призначені контейнерному об'єкту (наприклад, каталогу), то їх можуть успадковувати всі вкладені об'єкти (каталоги та файли). Успадкування можна обмежити під час задання прав.

Кожен список ACL складається з окремих елементів **ACE** (Access Control Entry). ACE визначає права доступу для окремого користувача або групи. Є три типи ACE:

• *Access Allowed* – дозволяє доступ згідно з маскою доступу;

• *Access Denied* – забороняє доступ згідно з маскою доступу;

• *System Audit* – використовують для генерування повідомлень, які записують у журнал безпеки.

Крім типу, кожен ACE має маску доступу – перелік наявних прав доступу. Конкретні права у ньому можуть залежати від типу об'єкта (*специфічні типи*) та не залежати від нього (стандартні типи). Набори специфічних та стандартних прав доступу формують *загальні (generic)* типи прав доступу.

Права доступу у разі звертання процесу в контексті певного користувача до певного об'єкта перевіряють так. Процес формує запит до об'єкта, тобто визначає потрібну маску доступу запиту – набір операцій, які він просить виконати з об'єктом. Ідентифікатори об'єкта, процесу та маска доступу надходять до монітора безпеки, який по черзі переглядає окремі ACE зі списку ACL об'єкта, керуючись такими правилами:

• якщо ACE не стосується цього користувача, то монітор його не розглядає, а переходить до наступного ACE;

• якщо ACE має тип Access Denied і його маска доступу збігається з маскою доступу запиту, запит відхиляють. Розгляд ACL припиняється;

• якщо доступ відхилено попереднього етапу, однак користувач вимагає прав ReadControl або write_dac, тоді, якщо користувач є власником об'єкта, доступ дозволяють;

• якщо ACE має тип Access Allowed і його маска доступу збігається з маскою запиту, доступ дозволяють і перегляд ACL припиняється;

• якщо ACL закінчився, а дозволу не було, запит відхиляють.

Контроль подій безпеки. WNT має гнучку систему, яка дає змогу простежувати події, пов'язані з системою безпеки. Конкретну конфігурацію подій визначає адміністратор системи (для опрацювання великого списку подій можуть бути потрібні значні системні ресурси). Розрізняють системні події та події, визначені застосуваннями. Їх реєструють у системному реєстрі. Вони мають імена та ідентифікатори, їх генерують відповідні програмні модулі.

Робочі групи та домени. WNT дає змогу згрупувати комп'ютери двома способами:

• з використанням робочих груп;

• з використанням доменів.

Робоча група – це найпростіший спосіб об'єднання комп'ютерів. Машини робочої групи підтримують власну політику безпеки та бази даних користувацьких бюджетів. Користувача мережі робочої групи розпізнають через його ім'я та пароль, які є перепусткою і на всі інші комп'ютери робочої групи. Використання механізму робочих груп доцільне у невеликих мережах, де проблеми безпеки та обмеження доступу не мають великого значення.

Домен – це група серверів, що провадять спільну політику безпеки та поділяють бази даних користувацьких бюджетів. Один з комп'ютерів (найчастіше під WNT Server) є головним контролером домену **PDC** (Primary Domain Controller). Він зберігає централізовані бази даних бюджетів усього домену і може виконувати розпізнавання. Для більшої надійності інформація дублюється на інших серверах – вторинних контролерах домену **BDC** (Backup Domain Controller), що також можуть вести розпізнавання користувача. Вони заміняють первинний контролер, якщо той виходить з ладу. Користувач мережі реєструється один раз, його розпізнає один з контролерів домену.

Якщо мережа достатньо велика (понад 10000 користувачів), то один PDC більше не може підтримувати базу бюджетів. У системі доводиться створювати кілька доменів та задавати відношення між ними. Між двома доменами можуть бути налаштовані довірчі відносини. Домен, що довіряє (довіритель) іншому домену (довірений домен), дає змогу користувачам довіреного домену користуватися його ресурсами, навіть якщо ці користувачі не мають у домені-довірителі бюджету. Довірений домен передає домену-довірителю інформацію про групи та користувачів, розпізнаних у ньому.

У мережі з багатьма доменами відносини довіри потрібно задавати явно. Якщо домен *A* довіряє домену *B*, це не означає що домен *B* довіряє домену *A*. Крім того, відносини довіри не є транзитивними: якщо домен *A* довіряє домену *B*, а *B* довіряє *C*, це не означає, що *A* довіряє *C*.

Використання довірчих відносин між доменами дає змогу визначати користувацькі бюджети тільки один раз – у довіреному домені.

Отже, як робочі групи, так і домени є 'пласкими' структурами. Фахівці-практики вважають, що адміністрування доменних структур невиправдано складне. Фірма Microsoft планує перейти до ієрархічних систем групування комп'ютерів, які добре зарекомендували себе в службах мережевих каталогів NDS та X.500 (див. розділ 23). У майбутньому групування комп'ютерів треба зінтегрувати зі службою каталогів.

35.5. Особливості реалізації мережевих функцій у Windows NT 5

ОС WNT 5 призначена для використання не тільки в малих та середніх підприємствах, а і в великих корпораціях. Тому в цій системі поліпшені можливості багатопроцесорного опрацювання, введена підтримка кластерних вирішень. Однак найважливішим є реалізація нової служби каталогів – *Active Directory (AD)*. Розглянемо особливості AD порівняно з найпотужнішою службою каталогів NDS фірми Novell (див. розділ 23).

Служба AD реалізує збереження всіх метаданих корпоративної мережі в єдиній базі даних. За її допомогою переходять від пласкої системи організації мережі до ієрархічної. Головна

перевага AD перед NDS – це тісна інтеграція цієї служби з застосуваннями Windows. Наприклад, в AD можна зберігати персональні конфігураційні дані. Елементом AD є структура розподіленої файлової системи, що дає змогу автоматизувати реплікацію даних на резервні сервери.

NDS логічно розподіляє дані на рівні контейнерів, даючи змогу реплікувати довільну комбінацію об'єктів-підрозділів (OU). Загальна кількість резервних серверів може бути меншою від кількості контейнерів. В AD мінімальним контейнером є домен.

AD, на відміну від NDS, не дає змоги керувати правами доступу до одного об'єкта. Можна задавати права доступу тільки для ресурсів певного типу, певної властивості, об'єктів певного типу, групи властивостей. За OU в AD не закріплені права доступу, їх використовують тільки для організації даних. Політика безпеки ведеться через групи.

AD дає змогу організувати транзитивні двонапрямлені відношення між доменами. Однак, на відміну від NDS, адміністративні права через відношення не передаються. Не підтримується й успадкування прав, їх треба призначати у кожному вкладеному домені. Така схема успадкування називається статичною, на відміну від динамічного успадкування, реалізованого в NDS. Статичне успадкування складніше в адмініструванні, а динамічне потребує більших витрат ресурсів під час роботи системи.

ОС WNT 5 дає змогу задавати якість обслуговування в мережах, підтримує протокол RSVP. В ОС уведені модулі шифрування на рівні файлової системи, підтримується система Kerberos, мережеві протоколи з поліпшеним захистом PPTP/L2TP, IPSec.

У WNT 5 розширена підтримка стека TCP/IP, введена динамічна версія DNS (DDNS), у якій DNS-таблиці розширюються автоматично з появою нових гостів. Поліпшена взаємодія з Novell та Unix, наприклад, підтримується korn-shell та 25 базових команд Unix.

Бібліографія та джерела

1. Администрирование сети Microsoft Windows NT. Учеб. курс.-М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd", 1997.
2. *Борисов В.* Сетевые службы Windows NT 5 // Компьютерпресс. 1998. № 10.
3. *Кастер Х.* Основы Windows NT и NTFS. М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd", 1996.
4. *Ноулс А.* Windows NT 4 для профессионалов. СПб.: Питер Ком, 1998.
5. *Перкинс Ч., Стриб М.* NT Workstation. Учеб. руководство для специалистов MCSE. М.: Лори, 1997.
6. *Рассел И, Кроуфорд Ш.* Эффективная работа с Microsoft Windows NT Server версия 4.0. СПб.: Питер, 1998.
7. Ресурсы Windows NT. СПб.: BHV, 1995.
8. *Рули Д.* Сети Windows NT 4.0. К.:BHV, 1998.
9. Сетевые средства Windows NT. СПб.: BHV, 1996.

ОГЛЯД МЕРЕЖЕВИХ ПРОДУКТІВ ФІРМИ NOVELL

Розділ 36

Продукти Novell. Загальний підхід та системні вирішення. Класифікація мережевих продуктів. Повномасштабні операційні системи. Порівняння ОС Netware 2.2, 3.11, 3.12, 4.1, 4.11. Засоби приєднання до інших платформ. Бази даних. Засоби електронної пошти. Підтримки робочих груп. Засоби навчання.

Фірма Novell сьогодні є однією з найпотужніших та найвпливовіших з випуску мережевих ОС. Подібно до інших компаній Novell розробила велику кількість різноманітних продуктів, об'єднаних єдиною архітектурою та сумісних між собою. Орієнтуватися в цих продуктах – це вміти вибирати потрібну конфігурацію відповідно до власних потреб.

Від початку фірма поставила собі за мету створення продуктів, які є максимально сумісними, підтримують та співпрацюють з продуктами інших фірм. Продукти Novell підтримують понад 100 різних топологій мереж та адаптерів.

Водночас операційні системи Novell оптимізовані в напрямі забезпечення максимальної продуктивності мережі. У них використано низку нових технічних та апаратно-програмних вирішень.

Сьогодні ОС Netware є найпродуктивнішими, швидкими в роботі та простими в обслуговуванні.

Технічні та системні вирішення:

- ядро системи дає змогу реалізувати багатозадачне обслуговування;
- елеваторне шукання;
- кешування диска;
- фонове записування на диск;
- індексування таблиць розміщення файлу. Якщо на сервері зберігаються файли, розмір яких перевищує 2 Мб, FAT індексується, забезпечуючи швидке шукання.

Засоби забезпечення надійності:

- перевірка читанням після кожного записування;
- дублювання каталогів; зберігається копія кореневого каталогу;
- можна дублювати диск сервера; два сервери приєднують паралельно; якщо один з них вийде з ладу, доступним є інший з цією ж інформацією;
- дублювання FAT; підтримується робота з обома копіями FAT.

Система безпеки та захисту діє на рівнях:

- облікової інформації про користувачів;
- паролів;
- каталогів;

• файлів;
• міжмережевого захисту.

Файлова система. Для прискорення доступу та гарантування безпеки даних Novell використовує власну файлову систему.

Архітектурні вирішення. У версіях мережевих операційних систем Novell, призначених для великих мереж, уперше реалізована концепція розподілених обчислень (досі використовували підхід робочих груп). У цьому підході конкретні функції та ресурси жорстко закріплені за конкретними серверами. Таке жорстке прив'язання зручне для малих мереж, проте у великих мережах з кількома десятками чи сотнями станцій обмежує свободу дій користувачів та адміністратора. У концепції розподілених обчислень усі ресурси об'єднані в одну логічну мережу. Платформою, яка забезпечує виконання запиту, тут є сама мережа, а не сервери. Сервісні функції в такій мережі розподілені по всій мережі (децентралізовані). Прикладні програми, які трактують мережу як єдину одиницю обслуговування, називаються розподіленими.

Концепція розподілених обчислень реалізована в архітектурі **NICA** (Novell Integrated Computing Architecture).

Продукти Novell підтримують багато різних апаратних, програмних та комунікаційних платформ. Фірма Novell постачає велику кількість додаткових програмних блоків, які конфігурують у єдину систему. Ці блоки оформлені у вигляді **NLM-** (Netware Loadable Module) **модулів**.

Фірма Novell першою запропонувала функціонально достатньо повну та потужну комерційну службу каталогів (NDS).

Усі продукти Novell можна умовно розділити на такі групи:
• повномасштабні операційні системи: Personal Netware , Novell Netware 2.2, 3.11, 3.12, 4.x, 4.11;
• засоби приєднання до інших мереж та платформ;
• засоби керування мережею та мережеметрії;
• засоби підтримки діяльності робочих груп;
• керування базами даних у середовищі 'клієнт–сервер';
• поштової служби;
• навчання.

Розглянемо детальніше окремі категорії продуктів Novell.

Операційні системи Novell.

Personal Netware з'явилася у 1993 р. як дешева однорангова ОС. Вона працює з DOS або Windows і об'єднує від 2 до 25 користувачів, пропонуючи їм базовий сервіс – сумісне використання програм, файлів, принтерів. Кожен комп'ютер можна сконфігурувати як клієнт, сервер або як те і те разом. Використана проста адміністративна система з трьома правами доступу. Значною перевагою Personal Netware є сумісність з потужнішими системами Novell Netware 2.2, 3.11, можливість плавного переходу між ними та одночасного використання обох.

Netware v.2.2. Операційна система Netware v.2.2 – це повнофункціональна мережева ОС для малих компаній та груп користувачів (кількість користувачів – від 5 до 100). Вона дає змогу станціям DOS, Macintosh, Windows, OS/2 приєднатися до серверів мережі. У Netware v.2.2 реалізовано головні механізми підвищення надійності, описані вище. Якщо сервер друкування сконфігурований у мережі, він підтримує до 16 мережевих принтерів.

Netware v.3.11, 3.12. ОС Netware v.3.11 та удосконалена Netware v.3.12 призначені для потужніших мереж, які можуть об'єднувати від 10 до 250 користувачів на середніх та великих підприємствах. Вона дає змогу робочим станціям під DOS, Macintosh, Windows, OS/2 та Unix працювати з серверами мережі. Підтримує не тільки протоколи SPX/IPX, але й TCP/IP, які використовують у мережах Unix.

Netware 4.0 є удосконаленням технології розподілених обчислень. Її використовують в організаціях, які бажають об'єднати кілька своїх локальних мереж у єдину корпоративну, організовує доступ та керування сервером v.3.11, 3.12. Підтримує 5–1000 користувачів.

Netware SFTIII – спеціальний варіант операційної системи, який підтримує роботу двох дзеркальних файл-серверів. Його використовують в організаціях, де недопустиме навіть короткочасне вимкнення сервера.

Netware 4.1, 4.11 (Green river), Intranetware. Починаючи з версії 4.0, мережева ОС працює з деревом каталогів, у ній поліпшені засоби захисту системи на всіх рівнях. Система розрахована на корпоративний рівень і масштабується до систем з сотнями серверів і десятками тисяч клієнтів, розташованими по всьому світу. У версії 4.11 введена додаткова підтримка роботи з Internet та web-технологіями. У пакет Intranetware, крім Netware 4.11, увійшли додаткові засоби роботи з Internet (детальніша характеристика Netware 4.11 та Intranetware наведена в Д.36.1).

Програмні засоби приєднання до інших систем та платформ.

Netware for SAA v.1.3 призначена для приєднання до мережі головних машин IBM та AS/400. Її постачають у вигляді nlm-модуля. У комбінації з Netware LAN Workstation дає змогу користувачам DOS, Macintosh, Windows, OS/2 та Unix працювати з застосуваннями на головній машині IBM. Підтримує одночасно до 506 сесій.

Netware Access Services забезпечує одночасний доступ 16 різним віддаленим користувачам до ресурсів мережі через модеми, X.25-сполучення та мультиплексори. Віддалене опрацювання завдань. Доступ до файлів.

LAN Workplace for DOS дає змогу користувачам DOS та Windows працювати з системами протоколу TCP/IP. Наявність системи Netware у цьому випадку не обов'язкова.

LAN Workgroup гарантує користувачам мереж Netware, що працюють з DOS та Windows, прозорий доступ до мереж протоколу TCP/IP. Порівняно з LAN Workplace for DOS ця система дає додатковий сервіс, її використовують для більших систем.

NFS Gateway забезпечує доступ до Unix-файлів через NFS.

Flex/IP – двонапрямлений шлюз друкування між середовищами Netware та Unix. Він дає змогу передавати файли Unix-користувачам з середовища Netware.

Засоби керування мережею та мережеметрії.

Network Navigator дає змогу адміністраторам мереж персональних комп'ютерів керувати та конфігурувати середовище мережі.

Network Communication Services Manager – це побудована на Windows програма для моніторингу, керування мережею Netware, дає змогу використовувати Netware for SAA та великі машини. Програма оцінює ефективність мережі, даючи змогу адміністратору оптимізувати її.

Керування базами даних.

Засоби керування базами даних Novell розроблені для архітектури 'клієнт–сервер'. Продукт *Btrieve* значною мірою застарів.

Засоби підтримки діяльності робочих груп.

Одним з магістральних продуктів Novell є *Novell GroupWise* – інтегрований пакет підтримки діяльності робочих груп. Він містить функції електронної пошти і повинен замінити поштову службу MHS (детальніше про Novell GroupWise див. розділ 30).

Поштова служба.

Користувачі Netware, крім локальних поштових послуг, можуть користуватися глобальною поштовою службою *Netware Global MHS*. Свого часу вона була найрозвиненішою і давала змогу контактувати користувачам різних систем та платформ. Має вбудовану підтримку маршрутизації та сполучення робочих груп.

Послугами служби MHS можна скористатися для передавання не тільки текстових файлів, але й програм. Для передавання повідомлень використано технологію проміжного зберігання: повідомлення передаються між серверами MHS доти, доки не дійдуть до сервера, в межах дії якого є абонент-одержувач. Це спрощує процедуру маршрутизації. Крім того, можна визначити час, коли найдоцільніше передавати повідомлення. Програма MHS виконується на спеціальному сервері MHS.

MHS складається з двох програм. Перша – *Communication Manager* – функціонально відповідає рекомендаціям стандарту X.400 для агента передавання повідомлень, який переглядає чергу повідомлень, сортує їх та спрямовує за адресами. Адміністратор мережі може керувати передаванням повідомлень. Друга програма – *Transport Server* – пересилає повідомлення іншому комп'ютеру через модем, використовуючи SMF (Standard Message Format). Формат простої адреси:

користувач [.застосування]

де застосування – це програма електронної пошти, якій адресоване повідомлення.

Розширена MHS-адреса:

користувач [.застосування] @група. підприємство {закордонна адреса}.

Засоби навчання.

Крім паперової документації, фірма постачає на CD електронні навчальні продукти та Network Support Encyclopedia, що групує в єдину базу даних всю інформацію щодо інсталювання, роботи та підтримки мережі.

Бібліографія та джерела

1. Сердце сети – сетевая ОС // Compurterworld Киев. 1997. № 14(134).
2. *Пьянзин К.* Intranetware – Novell держит удар Microsoft // LAN Magazine. 1997. № 1.

ДОДАТОК ДО РОЗДІЛУ 36

Д.36.1. Нові можливості Intranetware та Netware 4.11

У жовтні 1996 р. Novell розробила пакет *Intranetware* – набір засобів для створення мереж Netware, intranet та доступу в Internet. В основі пакета є ОС Netware 4.11 (отже, Intranetware не є окремою ОС – це набір продуктів, у тому числі й ОС).

Склад пакета такий: ОС Netware 4.11, пакет *Netware/IP* (дає змогу будувати мережу Netware на базі протоколів TCP/IP), клієнти Netware, пакет *Novell Internet Access Server 4* (багатопротокольний маршрутизатор, шлюз IPX/IP, web-браузер Netscape), пакет *Novell FTP Services*, документація.

Netware 4.11 – це багатозадачна, багатопотокова ОС з вбудованою підтримкою багатопроцесорного опрацювання SMP та повною відмовостійкістю (SFT III). На відміну від попередньої версії ОС у ній різко збільшені вимоги до ємності оперативної пам'яті (було – 8 Мб, є мінімум 20, крім того, по 8 Мб на кожний гігабайт дискового простору, а також на додаткові продукти. На твердому диску система і документація займають 250 Мб).

Головні характеристики:

• ОС Netware 4.11 відповідає вимогам С2 для мережевої конфігурації. Працює в стандартній конфігурації або в конфігурації з посиленим захистом. Навіть стандартна конфігурація ліпше захищена, ніж попередні версії Netware;

• Netware 4.11 – це перша система з підтримкою Plug and Play. Однак ця функція ще недостаньо розвинута порівняно з W95;

• у складі Netware 4.11 є *Netbasic* – командний процесор, що дає змогу створювати досить складні програми (інтерпретатор, не створює nlm-модулів). Його можна використовувати і для програмування web-сервера;

• ОС більше не підтримує MHS і орієнтована на GroupWise;

• є програмні засоби, що дають змогу керувати застосуваннями з консолі адміністратора. Вони складаються з менеджера застосувань (*Netware Application Manager* (*NAM*)) та середовища їх запуску (*Netware Application Launcher* (*NAL*)). З використанням NAM адміністратор створює в певному контексті NDS-об'єкт – Application – і запускає застосування, використовуючи його. Додаткова можливість – автоматичне оновлення програм клієнта під час реєстрації користувачів у мережі. Є змога простежити ліцензії у мережі;

• забезпечує швидке монтування та демонтування томів, поліпшені засоби поновлення роботи сервера після збою. Реалізовано поступовий перехід від протоколів SAP/RIP до протоколу NLSP, який налагоджується в Netware 4.11 за замовчуванням. Цей протокол значно зменшує трафік між серверами у великій мережі;

• для підтримки web-технологій є високопродуктивний web-сервер *Netware Web-Server 2.51*, однак у ньому нема редактора HTML. Користувачі одержують доступ до бази NDS;

• програма *Netware/IP 2.2.* дає змогу застосовувати в мережах Netware стек TCP/IP. Містить служби DNS, DHCP.

Клієнти Netware такі:

• vlm-клієнт для DOS/Windows;
• vlm-клієнт для DOS/Windows під IP;
• 32-розрядний клієнт для DOS/Windows;
• 32-розрядний клієнт для W95;
• клієнт OS/2;
• клієнт Macintosh.

Клієнт NT є в бета-версії. За допомогою засобів адміністрування можна працювати одночасно з кількома деревами NDS. У 32-розрядних клієнтах DOS/Windows та W95 задіяна технологія, яка дає змогу значно зменшити вимоги до пам'яті в першому мегабайті (до 3 Кб).

У ОС запропоновано три варіанти доступу до web-серверів:

• завантаження на кожний клієнт мережі стеків SPX/IPX та TCP/IP. У мережі одночасно працюють два протокольні стеки. Забезпечується незалежність і простота налагодження обох мереж, однак на клієнті використовується більше пам'яті;

• доступ клієнтів SPX/IPX до мережі TCP/IP через шлюз IPX/IP. На клієнтських машинах реалізовано тільки стек SPX/IPX. Схема має більшу захищеність і меншу надійність доступу до мережі TCP/IP (її визначає працездатність шлюзу);

• використання в мережі Netware протоколів IP. У клієнтів встановлюють тільки стек TCP/IP. На серверах використовують продукт Netware/IP. Однак у цьому випадку можливі труднощі перенесення всіх серверів на Netware/IP, деякі мережеві застосування Netware конфліктують з ним.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОС NOVELL NETWARE 4.x

Історія виникнення операційної системи Novell Netware 4.x. Головні архітектурні вирішення та відмінності від ОС Novell Netware 3.11. Служба каталогів та файлова система. Типи об'єктів. Поняття контексту. Керування розділами та часом. Головні принципи організації роботи сервера. Модулі nlm.

Операційна мережева система Novell Netware 4 з'явилася на ринку у 1994 р. Початкова версія 4.0 мала багато недоліків, тому менше ніж через рік створено нову, стабільну версію Novell Netware 4.1. Порівняно з ОС Novell Netware 3.11 версія 4.x містить низку принципово нових концептуальних стратегічних вирішень. Вона призначена для особливо великих корпорацій і може охоплювати весь світ. Водночас ця ОС досить гнучка та зручна в користуванні і для малих та середніх фірм з перспективою розвитку. Novell Netware 4.x розрахована на 10 і більше робочих станцій.

В основі архітектурної концепції Novell Netware 4.x є *Служба каталогів Netware* ***NDS*** *(Netware Directory Services)* (див. розділ 23). Згідно з цією концепцією всі ресурси мережі – це об'єкти, занесені в спеціальну розподілену базу даних – Netware Directory Database (NDD). Визначено різні можливі типи об'єктів: користувач, сервер, том, група користувачів та ін. Ці об'єкти згруповані в ієрархічному дереві, яке відображає їхню взаємну підпорядкованість. Кожен об'єкт конкретного типу має особливий набір властивостей та їхніх значень. Зокрема, об'єкт типу *користувач* має такі властивості: ім'я, пароль, поштову адресу, адресу електронної пошти, номер телефону, належність до груп користувачів та ін. Людина, що працює в мережі, може аналізувати властивості об'єктів у NDS.

На відміну від Novell Netware 4.x, версія 3.11 не має NDS. Кожен користувач на початку роботи приєднується (bind) до одного сервера і, отже, може працювати одночасно тільки з одним сервером. База даних, яка зберігає інформацію про прикріплення користувача до сервера, в Novell Netware 3.11 називається *bindary*. Користувач Novell Netware 4.x приєднується відразу до цілого дерева об'єктів і може працювати з ними одночасно. Серед цих об'єктів є і сервери.

Можна сказати, що Novell Netware 4.x складається з двох головних підсистем: NDS та файлової системи (рис. 37.1).

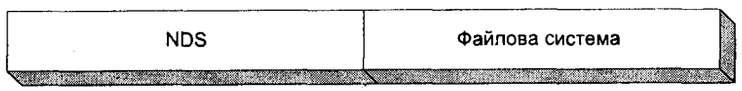


Рис. 37.1. Підсистеми Novell Netware 4.x.

Кожна з цих підсистем має свої механізми захисту та керування, тоді як Novell Netware 3.11 охоплює тільки файлову систему.

NDS діє на структурі об'єктів, яку називають *деревом каталогів*. Вона має три структурні типи об'єктів:

- кореневий – *Root*;
- контейнерний – *Container object*;
- кінцевий – *Leaf object*.

Кожне дерево має тільки один кореневий об'єкт. Йому умовно відповідає об'єкт – весь світ. Контейнерні об'єкти містять інші об'єкти, а кінцеві є головними, з ними працюють (див. розділ 23).

37.1. Поняття контексту

Контекстом називається шлях від заданої позиції в дереві до його кореня. Щоб працювати з деревом каталогів, обов'язково треба знати свій контекст. Правила записування контексту розглянемо на прикладах (див. рис. 23.5) (окремі гілки на шляху розділяють крапками):

cn=student.ou=icm.ou=cf.o=techn_univ.c=ua для користувача student

Рівні контексту задавати необов'язково. Однак, якщо визначено рівень С, то позначати рівні треба. Наприклад:

а) student.cf.techn_univ для користувача student;
б) admin.cf.techn_univ для користувача admin;
в) rector.techn_univ для користувача rector;

Працюючи з деревом каталогів і перебуваючи в конкретному місці дерева, потрібні об'єкти завжди шукають спочатку в цьому контейнерному об'єкті. Наприклад, для шукання об'єкта student треба було перейти в контекст ou=icm.ou=cf.ou=techn_univ.

З іншого боку, права користувача, визначеного в дереві каталогів 'вище' автоматично поширюються на всі об'єкти, що є нижче по дереву. Наприклад, права користувача admin поширюються на об'єкти в ou=icm.

Якщо треба блокувати таке успадкування, користувач з відповідними повноваженнями може використати *Фільтр успадкованих прав* ***IRF*** *(Inherited rights filter)*.

37.2. Права доступу

У Netware 4.x визначені такі чотири типи прав:

- **на об'єкт** – права на об'єкт як одне ціле; дають змогу створювати, знищувати та переглядати об'єкти;

- **на властивість** – права на властивість об'єкта; регулюють доступ до певних властивостей об'єкта;
- **на каталог** – дають змогу маніпулювати з конкретним каталогом;
- **на файл** – регулюють доступ до певного файлу.

Перші два права стосуються NDS, а решта поширюються на файлову систему. Інформація про права доступу до кожного об'єкта зберігається в його властивості *Список керування доступом ACL*.

В операційній системі Novell Netware 3.11 є один визначений користувач – *Supervisor*, який має всі права для керування мережею. Його не можна знищити чи перейменувати або обмежити в правах. У Novell Netware 4.x кількість адміністраторів може бути довільною. Під час інсталювання мережі створюють одного користувача з іменем *Admin* та правами адміністратора, згодом його можна перейменувати, а також створити інших користувачів з правами адміністратора на різних рівнях дерева. Кожного користувача-адміністратора можна знищити, якщо після цього залишиться хоча б один адміністратор. Отже, Novell Netware 4.x допускає як централізоване, так і децентралізоване керування, тоді як Novell Netware 3.11 – тільки централізоване.

37.3. Керування розділами бази даних об'єктів NDS

Як зазначено, інформація про ресурси мережі зберігається в розподіленій базі даних. Окремі частини цієї бази є на різних серверах. Водночас для користувача ця база даних повинна виглядати як єдине ціле. З метою збільшити надійність, доступність інформації про NDS-об'єкти, зменшити керівні інформаційні потоки в мережі Novell Netware 4.0 вводять об'єкт *розділ* та механізм керування ним.

Розділ *(Partition)* – це логічний об'єкт, що містить інформацію про контейнерний об'єкт, який охоплює деяку логічну частину дерева каталогів. У складі такого контейнерного об'єкта обов'язково повинен бути сервер. Розділ містить інформацію про структуру та зміст відповідної частини дерева, однак не має інформації про файлову систему. Розділи створюють під час інсталювання та коректують під час роботи мережі утилітами *Nwadmin* та *Partmgr*. Приклади поділу дерева на розділи показані на рис. 37.2. З метою збільшити швидкодію роботи системи та її надійність роблять копії (репліки) кожного розділу. Кожен розділ повинен мати хоча б дві копії. Копії одного розділу обов'язково зберігають на різних серверах (пор. з організацією збереження інформації в базі даних DNS, розділ 13). Визначено три типи копій.

- *Головна (Master)* є завжди в одному примірнику, її використовують для керування мережею, її не можна знищити чи модифікувати за допомогою утиліт;
- *Читання-записування (Read/Write)*. Її можна редагувати. Крім того, можна поміняти місцями статуси копій Master та Read/Write так, що копія Master стане Read/Write, і навпаки;
- *Тільки для читання (Read Only)*.

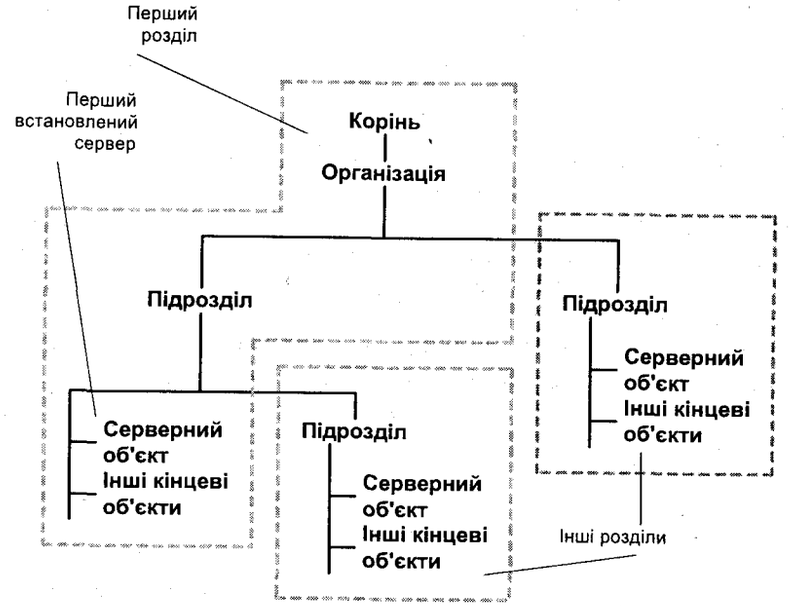


Рис. 37.2. Поділ дерева каталогів на розділи.

37.4. Керування часом

Мережа операційної системи Novell Netware 4.x може мати велику географічну площу і містити об'єкти, що розташовані у різних часових зонах. Однак вона повинна працювати як єдиний механізм, тому для всіх об'єктів потрібен єдиний час. Кожен сервер є водночас і сервером часу.

Визначено чотири типи серверів часу:

• **єдиний довідковий** (Single Reference Time Server). Задає час для всієї мережі. Його використовують за замовчуванням та в невеликих (зокрема з одним сервером) мережах, проте таке вирішення ненадійне;

• **довідковий** (Reference Time Server). Він має зовнішній годинник. Разом з іншими довідковими серверами часу та первинними серверами часу бере участь у голосуванні для визначення єдиного мережевого часу. Не налаштовує свій годинник за результатами голосування;

• **первинний** (Primary Time Server). Бере участь у голосуванні, налаштовує свій годинник за результатами голосування;

• **вторинний** (Secondary Time Server). Не бере участі у голосуванні та налаштовує свій годинник за результатами голосування.

37.5. Головні принципи організації роботи сервера Novell Netware

За організацією процесу опрацювання інформації операційні системи можна розділити на ОС загального призначення та спеціалізовані. Перші не передбачають орієнтації застосувань на внутрішню структуру ОС. Вони працюють з розподілом пам'яті та інших ресурсів комп'ютера між усіма процесами (принцип розподілу часу). Цей підхід забезпечує високу стійкість та надійність, однак знижує швидкодію, гнучкість побудови та функціонування застосувань, і, як наслідок, – ефективність використання ресурсу. До систем з розподілом часу належать такі популярні ОС, як Unix та Windows NT.

Netware – це спеціалізована мережева ОС, орієнтована на максимальну ефективність використання апаратних ресурсів, належить до ОС, що працюють у невитісняючому режимі та не займаються розподілом часу ЦП. Netware складається з невеликого ядра, що виконує обмежене коло функцій, та завантажувальних модулів *nlm (Netware Loadable Modules)* (рис. 37.3). Ці модулі виконують функції операційної системи. Зокрема, в Netware 4.x є близько 1000 nlm-модулів.

В ОС Netware застосування самі повинні передавати керування одне одному. Якщо в некоректному модулі не передбачено передавання керування, він може займати центральний процесор невизначено тривалий час. Тому всі nlm-модулі повинні пройти тестування в лабораторіях Novell (У Netware 4 передбачено захист від некоректних модулів інших фірм – див. розділ 41). Модулі, що успішно пройшли тестування, мають позначку *Yes, it runs with Netware*. Наприклад, жодний з потоків не може захоплювати процесор більше ніж на 10 мс. Відсутність витіснення дає змогу підвищити ефективність системи, оскільки в цьому разі зникає функція диспетчеризації та відповідні процеси. Невитісняючий характер Netware дає змогу робити паузи у природні моменти (наприклад, очікування доступу до бази даних або набирання номера АТС).

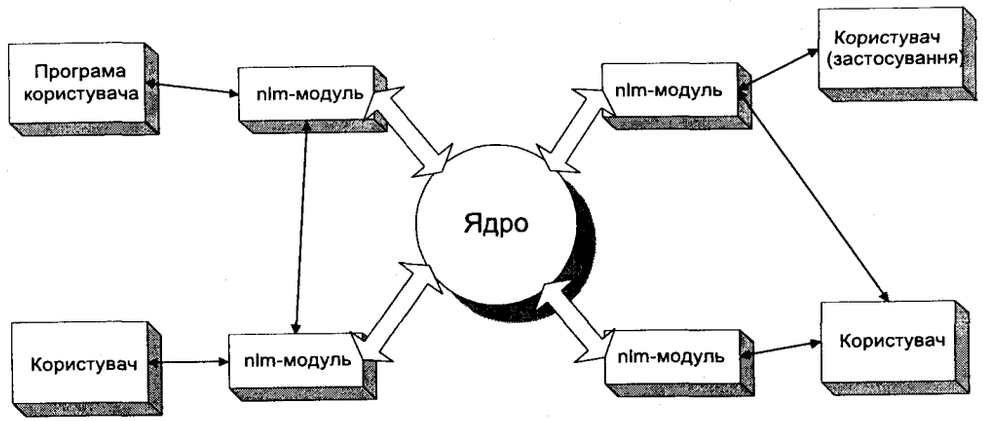


Рис 37.3. Робота ОС Novell.

Кожен nlm-модуль обслуговує запити робочих станцій і сам звертається до ресурсів через ядро системи. Описати роботу системи можна за допомогою механізму потоків (thread). *Потік* – це послідовність команд, що її виконує процесор. Кожен запит робочої станції формує окремий потік. Один і той же nlm може генерувати кілька потоків. Усі активні потоки розміщені в одній із чотирьох черг: *RunList*, *DelayWorkToDoList*, *LowPriority*, *WorkToDoList*. Операційна система створює свій робочий потік, який має найвищий пріоритет. У черзі *WorkToDoList* розміщені короткі завдання, які потрібно швидко виконати. Робочий потік виконує кілька завдань з цієї черги, після чого керування переходить до звичайних потоків з черги *RunList*, а сам робочий потік стає в кінець черги *RunList*.

Отже, *RunList* – це черга звичайних потоків. Новий потік стає у кінець черги, а перший у черзі виконується доти, доки не передасть керування наступному потоку.

У черзі *DelayWorkToDoList* розміщені звичайні потоки, що починають керувати тільки після того, як процесор опрацює визначену кількість потоків з інших черг. Потокам з черги *LowPriority* керування передається тільки тоді, коли всі інші черги порожні. Цю чергу використовують для розміщення фонових задач.

Оскільки трафік запитів проходить через nlm-модулі, то вони виконують функцію контролю трафіку та борються з вірусами.

Приклади nlm-модулів:

- cdrom.nlm – приєднання пристрою читання з компакт-дисків;
- router.nlm – програма маршрутизатора.

Бібліографія та джерела

1. *Бирер Д.* Внутренний мир Netware 4.1. К.: Диасофт, 1997.
2. *Лоренс Б.* Novell Netware 4.1 в подлиннике. СПб.: BHV, 1996.
3. *Крейнес А.* Очереди без конфликтов // Сети. 1996. № 4.
4. *Титтел Є., Коннор Д.* Netware для чайников. К.: Диалектика, 1995.
5. *Ценк А.* Novell Netware 4.x. К.: BHV, 1996.

НАЛАШТУВАННЯ СЕРВЕРА ОС NOVELL NETWARE 4.x

Загальна характеристика етапів налаштування. Планування дерева каталогів. Вимоги до сервера. Підготовка твердого диска. Вибір драйвера диска. Формування томів. Встановлення драйвера адаптерної плати. Інсталювання NDS. Визначення контексту сервера. Файли startup.ncf та autoexec.ncf, їхнє призначення, структура та приклади.

Процедури налаштування операційної системи суттєво відрізняються для сервера та робочої станції Novell 4.x. У цьому розділі ми розглянемо процедуру налаштування системи для сервера.

Процедуру налаштування операційної системи Novell Netware 4.x для зручності можна розділити на такі етапи:

- планування дерева каталогів;
- попередній аналіз, оцінка технічних параметрів та підготовка робочого місця;
- формування диска, файлової системи та інсталювання адаптера;
- налаштування NDS;
- формування та коригування файлів startup.ncf та autoexec.ncf;
- налаштування додаткових продуктів.

38.1. Планування дерева каталогів

Перед початком налаштування нового сервера Novell Netware 4.x треба спланувати структуру дерева каталогів. Цей етап особливо важливий, якщо сервер, який інсталюють, перший у дереві. Структура дерева каталогів повинна забезпечити:

- стійкість до відмов;
- зменшення інформаційних потоків;
- зручність керування.

Вона може відображати організаційну структуру підприємства або структуру тем, робочих груп тощо. Треба також дати ім'я дереву, яке створюють, продумати систему найменування користувачів, а також систему безпеки та адміністрування.

Для найменування користувачів рекомендують складати ім'я з ініціала та прізвища. Наприклад, *CSmith*, *VPasitchnyk*. Така система досить інформативна та запобігає дублюванню імен. Для системи адміністрування та безпеки треба вибрати між централізованим та децентралізованим адмініструванням, визначити попередньо паролі та права доступу.

38.2. Попередній аналіз технічних параметрів та підготовка робочого місця

Обов'язковою умовою налаштування сервера є наявність комп'ютера з вмонтованою платою адаптера мережі. Кожен сервер мережі потрібно приєднувати до живлення через *джерело безперебійного живлення (Uninterrupted Power Supply – UPS).*

Комп'ютер для сервера Novell Netware 4.x повинен мати низку значень параметрів. Ці вимоги стосуються головно ємностей оперативної пам'яті та твердого диска.

Щодо оперативної пам'яті, то складові частини для розрахунку потрібної ємності такі:

• мінімальна базова – 6 Мб.

Помножте ємність диска на 0.008 і одержаний результат додайте до загальної суми. Наприклад, 200·0.008 = 1.6 Мб;

• для завантаження додаткових продуктів Novell, таких як Netware for NFS, Btrieve, налаштування сервера друкування додайте ще 2 Мб пам'яті на кожен продукт;

• для збільшення швидкодії сервера виділіть ще 1–4 Мб для програмного кешу.

Отже, ємність оперативної пам'яті не може бути меншою ніж 8 Мб, а ємність твердого диска – меншою ніж 55 Мб.

Перед початком налаштування сервера треба проаналізувати низку технічних параметрів комп'ютера:

• архітектуру комп'ютера та тип системної шини (ISA, MCA, EISA, PCI);

• тип контролера твердого диска (AT, IDE, ESDI, SCSI);

• тип адаптера локальної мережі, номер переривання та адресні параметри.

Номер переривання, адресні параметри адаптера не можуть бути зайняті іншими компонентами апаратного забезпечення комп'ютера. Інакше налаштування ОС не відбудеться або в подальшому у системі виникатимуть незрозумілі збої. Номери переривань та адреси блоків пам'яті, що використовуються, можна виявити за допомогою утиліт Sysinfo, CheckIt та ін.

Усі параметри треба занести в окрему форму, яку заповнюють під час налаштування сервера (див. Д.38.1) і зберігають протягом усього часу його експлуатації.

38.3. Формування диска та файлової системи

Процес формування диска та файлової системи для зручності опишемо у вигляді окремих задач.

1. Форматування нижнього рівня для диска.

Диск форматують на нижньому рівні засобами DOS, через Setup або спеціальними утилітами, перевіряючи та позначаючи всі погані сектори.

Лабораторії фірми Novell на комп'ютерах вичерпно тестують поверхню твердого диска, протягом трьох діб безперервно виконуючи операції записування-читання. Комп'ютер, який успішно пройшов такий тест, одержує відповідний сертифікат і право називатися сервером, що сертифікований Novell'ом. Однак сьогодні фірма Novell не вимагає сертифікування всіх серверів. Відповідна програма тесту поверхні з назвою Compsurf є в пакеті інсталяційних програм.

2. Формування завантажувального розділу DOS.

На диску за допомогою утиліти DOS fdisk формують завантажувальний розділ. Власне з нього відбуватиметься в подальшому первинне завантаження сервера під час увімкнення. На розділ копіюють файли DOS. Мінімальна ємність розділу – 5 Мб. Решта ємності твердого диска є вільною.

3. Запуск програми налаштування сервера.

Для налаштування сервера треба запустити програму install.bat. Це, як звичайно, пакетний командний файл, який запускає спеціальну інсталяційну програму nwnstll.exe, що функціонально еквівалентна утиліті сервера install.nlm. З використанням програми nwnstll.nlm виконують таку послідовність задач:

• вибирають та завантажують драйвер твердого диска;

• на вільному місці диска створюють розділ Netware;

• створюють та монтують томи;

• копіюють системні файли;

• обирають та завантажують драйвер мережевого адаптера;

• налаштовують NDS;

• формують та редагують файли startup.ncf та autoexec.ncf;

• налаштовують додаткові програмні продукти.

4. Вибір та завантаження драйвера диска.

Вибір драйвера твердого диска залежить від архітектури комп'ютера та типу контролера диска. Деякі найпоширеніші драйвери наведені у табл. 38.1.

Таблиця 38.1. Драйвери твердого диска

Архітектура	Контролер	Драйвер
ISA	AT IDE(ATA)	ISADISK IDE
MCA	ESDI IBMSCSI	PS2ESDI PS2SCSI
EISA	AT IDE(ATA)	ISADISK IDE

Потрібний драйвер вибирають зі списку драйверів, запропонованих програмою.

5. Створення розділу Netware.

Розділ Netware створюють автоматично (на всю вільну ємність диска) або вручну (на визначену ємність диска). Для кодування та відображення інформації в цьому розділі використовують коди та формати даних, які відрізняються від кодів та форматів інших операційних систем (DOS, Unix, OS/2), що додатково захищає інформацію від вірусів та несанкціонованого доступу. Частину розділу на цьому етапі виділяють для даних зі зіпсутих секторів (так звана *Hot Fix Area*, див. розділ 41). За замовчуванням вона займає 4% розділу. На цьому етапі налаштування цей відсоток можна змінити.

Розділ Netware показано на рис. 38.1.

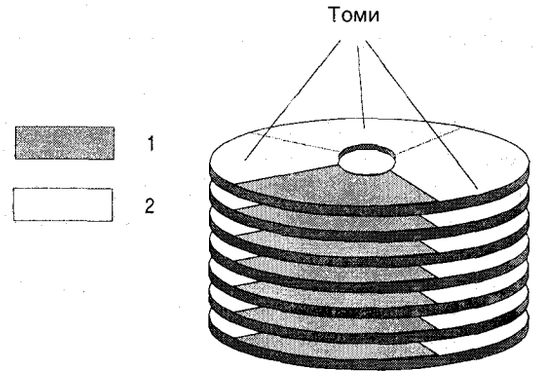


Рис. 38.1. Розподіл твердого диска в Netware. Розділи: *1* – Netware, *2* – DOS.

6. Формування томів.

Сформований розділ Netware треба розділити на томи. Один з томів є обов'язковим, на ньому зберігають системну інформацію. Його ім'я – *sys*. Для інших томів ім'я вибирають довільно. Максимальна кількість томів – 32. На цьому ж етапі задають розмір блоку (блок – це мінімальна адресована одиниця інформації, аналог кластера MS DOS). Розмір блоку автоматично обирається залежно від розміру тому (*наприклад, для тому розміром 0–31 Мб блок займає* 4 Кб, а для тому понад 2000 Мб – вже 64 Кб). Чим більший розмір блоку, тим потенційно менш ефективно використовується дисковий простір, чим менший розмір блоку, тим більше місця займають системні таблиці і довше триває шукання інформації. Формуючи томи, розмір блоку, визначений автоматично, можна змінити.

Під час формування томів кожному тому можна дозволити або заборонити два режими роботи.

• *Автоматичне стиснення файлів* дозволено або заборонено на рівні тому. Керування ж стисненням конкретних файлів під час роботи системи відбувається з використанням утиліти flag. Якщо стиснення заборонено на рівні тому, то стиснути окремі файли неможливо.

• *Раціональне використання блоків (block suballocation).* Механізм раціонального використання блоків дає змогу використати незаповнену файлом частину блоку.

7. Перевіряння ліцензійної інформації та копіювання системи.

На цьому етапі інсталяційна програма потребує встановлення дискети з ліцензією. Після перевіряння повноважень вона копіює системні файли з дистрибутива в розділ Netware. Для цього створюють каталоги system, public, login, mail.

8. Завантаження мережевого драйвера.

Програма налаштування виводить список назв мережевих адаптерів, з якого треба вибрати назву адаптера, встановленого на вашому комп'ютері. Після цього потрібно задати номер переривання та адресні параметри. Якщо номер переривання або адреса недопустимі, програма повідомляє про це і просить задати інші параметри. Потім задають тип *фрейму*, тобто тип кадру, який використовують для передавання даних. Як звичайно, цей тип відповідає типу локальної мережі (Ethernet, Token Ring, Arcnet та ін.)

Для мережі Ethernet доступні відразу два типи фреймів – Ethernet 802.2 та Ethernet 802.3 (див. розділ 15, Д.15.1).

Після налаштування мережевого драйвера програма налаштування сполучає драйвер з протоколом мережевого рівня *IPX (Inter Packet eXchange).* Тут також задають унікальну адресу сервера.

Програма налаштування дає змогу задати кілька драйверів для одного або кількох адаптерів, а також налаштувати кілька різних типів фреймів.

38.4. Налаштування NDS

Метою налаштування NDS є створення деякої початкової кількості об'єктів NDS та визначення їхніх головних параметрів. Для зручності цей етап також розділимо на окремі задачі.

1. Визначення імені дерева.

Після формування диска програма налаштування перевіряє наявність дерева каталогів і пропонує задати його ім'я. Нове ім'я дерева визначають обов'язково, якщо налаштований сервер є першим. В іншому випадку можна задати нове ім'я, розпочинаючи таким чином нове дерево, або приєднати сервер до наявного дерева.

Задаючи нове дерево, треба пам'ятати, що одночасно можна працювати тільки в одному дереві (у Novell Netware 4.1).

2.Визначення часових параметрів сервера.

Правильне налаштування внутрішнього часу сервера забезпечує часову цілісність мережі і потрібне для правильного її функціонування. Визначено такі часові параметри:

• тип сервера часу (див. розділ 37); якщо сервер є першим у мережі, єдиним прийнятним типом є *Single Reference time Server*;

• часова зона – задають як зміщення від UCT (Universal Coordinated Time);

• наявність переходу на літній час, тривалість періоду літнього часу, час зміщення.

3. Визначення контексту сервера та створення розділу БД NDS.

На цьому етапі налаштування задають ім'я організації та потрібну кількість підрозділів, в останньому з яких буде розміщено серверний об'єкт. Після визначення контексту сервера програма налаштування за замовчуванням визначає новий розділ БД NDS, розміщуючи Master-копію цього розділу на сервері, який налаштовують, а Read/Write – на інших серверах того ж контексту або в сервері найближчого сусіднього розділу.

У результаті налаштування NDS створюють такі об'єкти:

1) серверний, наприклад, icm_server;

2) томів, наприклад, icm_server_sys;

3) користувача з іменем admin, що має права адміністратора у контексті сервера.

Приклад структури дерева після налаштування сервера показано на рис. 38.2.

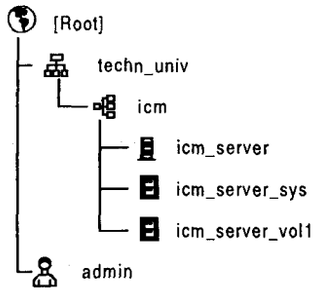


Рис. 38.2. Структура дерева після налаштування сервера.

38.5. Формування та корекція файлів startup.ncf та autoexec.ncf

Файли startup.ncf та autoexec.ncf – це текстові командні файли, які формуються в процесі налаштування сервера і згодом використовуються кожного разу під час завантаження сервера. Можна сказати, що результатом налаштування сервера і є формування файлів startup.ncf та autoexec.ncf. Водночас ці файли є звичайними текстовими файлами і їх можна коректувати текстовим редактором. Щоб зрозуміти їхнє призначення, розглянемо процес щоденного завантаження сервера.

Під час вмикання комп'ютера завантажується DOS з розділу DOS. Після цього треба відшукати та запустити програму server.exe, яка й завантажує сервер. Ця програма спочатку відшукує в розділі DOS файл startup.ncf та виконує його. Одним з обов'язкових елементів цього файлу є завантаження драйвера диска. Після цього *server.exe* монтує системний том SYS.

Змонтувати том – це зробити його відомим для операційної системи. Під час монтування формують службові таблиці та заносять їх у пам'ять. Незмонтований том недоступний для користування. Водночас чим менше томів змонтовано, тим швидшим є доступ до даних, менше пам'яті зайнято службовою інформацією.

Після того, як системний том SYS змонтовано, програма server.exe читає з нього командний файл autoexec.ncf, який містить команди завантаження мережевого драйвера, приєднання до протоколів, інші команди конфігурації (приклад файлу autoexec.ncf з коментарями є наведений у Д.38.2).

Отже, startup.ncf і autoexec.ncf використовують для початкового завантаження системи. Вони містять команди, які керують цим завантаженням. Однак startup.ncf розміщено в розділі DOS і його головна функція – завантажити драйвер диска та зробити можливим монтування системного тому SYS та доступ до файлу autoexec.ncf, який розміщено в розділі Netware. Головні команди, що керують завантаженням ОС, записані в autoexec.ncf.

38.6. Налаштування додаткових продуктів Netware

Після налаштування головної частини операційної системи в autoexec.ncf можна записати команди завантаження додаткових продуктів Netware. Їх постачають у вигляді файлів з розширенням nlm.

Загалом розширення nlm мають і серверні утиліти та інші модулі, які завантажують під час роботи сервера командою load назва_модуля.nlm.

До додаткових продуктів Netware належать пакет роботи з базами даних Btrieve.nlm, програма керування сервером друкування Print.nlm та інші.

38.7. Післяінсталяційне використання програми налаштування

Зазначимо, що програму налаштування системи можна завантажити і після фактичного завершення процесу інсталювання, щоб змінити системні параметри. У цьому випадку треба завантажити модуль install.nlm і вибрати пункт меню *Maintenance/Selective install.* Тут можна змінити параметри завантаження драйвера диска та мережевої плати, налаштувати параметри томів та часові параметри, знову скопіювати системні файли і налаштувати додаткові продукти Netware.

Бібліографія та джерела

Ценк А. Novell Netware 4.x. К.: BHV, 1996.

ДОДАТКИ ДО РОЗДІЛУ 38

Д.38.1.Форма для записування параметрів налаштування сервера

Ім'я сервера _____ **Адреса IPX** _____
Модель/виробник сервера _____ **Ім'я дерева** _____
Тип сервера часу _____ **Часова зона** _____ **Зміщення від UCT** ____ **Вперед**
____ **Назад**
ОЗП (RAM): Базова _____ **Розширена** _____ **Всього** _____
Метод завантаження серевера: Тв. диск ☐ **Дискета 3.5"** ☐ **5.25"** ☐

Мережеві адаптери

Назва	Мережевий драйвер	Порт уведення/ виведення	Адреса пам'яті	IRQ	Канал DMA	Адреса станції/ вузла	Номер слота	Мережева адреса

Інші адаптери (зовнішні або внутрішні дискові контролери, SCSI-контролери, відеоадаптери)

Назва	Драйвер	Порт уведення/ виведення	Адреса пам'яті	IRQ	Канал DMA	SCSI адреса	Інша інформація

Тверді диски

Модель	Ємність	Дзеркально пов'язаний з #	Сегменти томів

Томи

Ім'я тому	Стиснення файлів		Використання блоків		Міграція даних		Ім'я області
	так	ні	так	ні	так	ні	

Д.38.2. Приклад змісту файлу autoexec.ncf

```
set Time Zone = MET-1 MEST ; Задається назва часової зони

set DayLight Savings Time Offset = 1:00:00 ; Зміщення часу під час уведення літнього часу

; початок та кінець літнього часу
set Start of Daylight Savings Time= (MARCH SUNDAY LAST 2:00:00 AM)
set End of Daylight Savings Time=(SEPTEMBER SUNDAY LAST 2:00:00 AM)

; тип часового сервера
set Default Time Server Type = SINGLE

; контекст для розміщення bindery та емуляції послуг Netware 3.11
set Bindary Context= OU=802_2.O=ASU

; ім'я файл-сервера
file server Name MARTA_SERVER

; мережева адреса сервера
IPX internal net 1994BD01

; завантаження драйвера адаптера з певними числовими параметрами для певного фрейму.
Завантаженому драйверу присвоюється ім'я.
load 3C503 port1=750 PORT=350 int=3 MEM=D8000 Frame=Ethernet_802.3
                                                NAME= 3C503_1E_802.3
; цей драйвер приєднується до програми обслуговування протоколу IPX. Задається унікальна
мережева адреса (15609373).
bind ipx to 3C503_1E_802.3 net 15609373

; тепер завантажимо той же драйвер, але з іншим фреймом та ім'ям
load 3C503 port1=750 PORT=350 int=3 MEM=D8000 Frame=Ethernet_802.2
                                                NAME= 3C503_1E_802.2

; приєднаємо його до IPX. Задається інша адреса, за якою надходитимуть кадри відповідно до
програми опрацювання кадрів фрейму Ethernet_802.2.
bind ipx to 3C503_1E_802.2 net  55409B63
```

НАЛАШТУВАННЯ ТА ПРИНЦИПИ ФУНКЦІОНУВАННЯ РОБОЧОЇ СТАНЦІЇ NOVELL NETWARE 4.x

Загальна характеристика програмного забезпечення робочої станції. Налаштування робочої станції. Структура та призначення файлу startnet.bat. Структура і головні функції запитувача DOS. Модулі vlm та їхнє призначення. Структура та призначення конфігураційного файлу net.cfg.

Характерною особливістю комп'ютерної мережі є те, що в ній одночасно можуть функціонувати різні операційні системи. Наприклад, на серверах працює ОС Novell Netware, а робочими станціями можуть керувати DOS, Windows, OS/2, Unix.

39.1. Налаштування робочої станції

Після налаштування сервера та для налаштування станцій мережі треба підготувати інсталяційні дискети. Це можна виконати або на сервері з використанням утиліти install.nlm, або в DOS, запустивши програму makedisk і позначивши дисковод. Наприклад,

```
makedisk a:
```

У результаті формуються чотири дискети, позначені WSDOS_1, WSWIN_1, WSDRV_1, WSDRV_2. Вони призначені відповідно для початкового налаштування DOS-станції, подальшого завантаження Windows-програм (якщо потрібно) та для завантаження драйверів.

На робочій станції з дискети WSDOS_1 запускають програму налаштування install.exe. Вона задає низку питань про каталог для налаштування ПЗ станції (за замовчуванням цей каталог називається nwclient), тип мережевого адаптера та його параметри. У цьому процес налаштування станції аналогічний до процесу налаштування сервера.

39.2. Структура та принципи роботи ПЗ робочої станції Novell Netware 3.11

Структура програмного забезпечення робочої станції ОС Novell Netware 3.11 показана на рис. 39.1.

Прикладна програма звертається з запитом до ресурсів операційної системи станції. Спеціальна резидентна програма netx.exe (редиректор) перехоплює запит та вирішує, кому його спрямувати для обслуговування – DOS-станції або в програму ipx.com і далі на сервер.

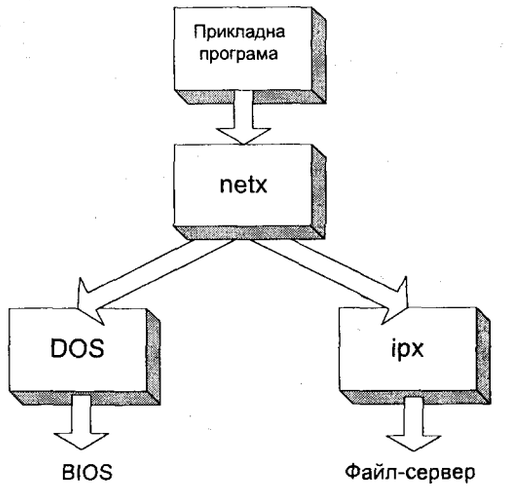


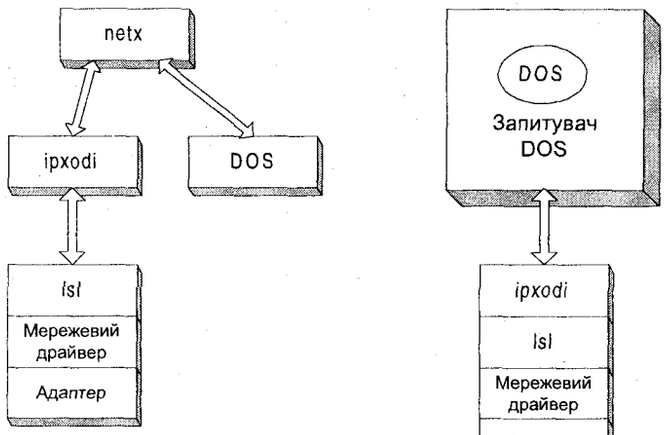
Рис. 39.1 Структура ПЗ робочої станції ОС Novell Netware 3.11.

У ОС Novell Netware програму netx *називають програмою мережевої оболонки, або по-англійськи shell. Назву* netx.exe *оболонка одержала, починаючи з версії 3.12. У попередніх версіях вона залежала від версії DOS:* net2, net3, net4, net5 *відповідно для DOS версій 2, 3, 4, 5. Є варіанти* netx *для завантаження у різні ділянки пам'яті. Це* emsnetx.exe *та* xmsnetx.exe *відповідно для різних типів пам'яті.*

Програма ipx.com містить програму формування пакета протоколу мережевого рівня IPX та драйвер мережевого адаптера. Оскільки можливих драйверів мережевих адаптерів є багато, програма ipx.com генерується кожного разу під час налаштування станції та задання типу і параметрів мережевого адаптера. Для цього в Novell 3.11 є спеціальна програма wssgen.exe.

39.3. Структура ПЗ робочої станції Novell Netware 4.x

В операційній системі Novell Netware 4.0 структура програмного забезпечення робочої станції зазнала суттєвих змін порівняно з версією 3.11. Це було зумовлене появою та впровадженням інтерфейсу специфікації *ODI*, точнішим дотриманням вимог еталонної моделі відкритих систем, потребою передавати одночасно пакети кількох різних протоколів. Структура ПЗ станції Novell Netware 4.x порівняно з Novell Netware 3.11 показана на рис. 39.2.



а *б*

Рис. 39.2 Структури ПЗ робочих станцій Novell Netware 3.11 (*а*) та Novell Netware 4.x (*б*).

Сьогодні є кілька загальноприйнятих специфікацій драйверів. Кожна з них дає змогу передавати інформацію незалежно від типу протоколу та мережевої плати. Відомо три такі специфікації:

- ***ODI** розроблена фірмою Novell, використовують у всіх мережевих програмних продуктах цієї фірми;*
- ***NDIS** розроблена в 1989 р. фірмами Microsoft та 3Com, використовують у LAN Manager, Windows for Workgroups, Windows NT, Windows 9x, Lantastic, Pathworks. Є 16-розрядний варіант NDIS, постійно резидентний у базовій пам'яті, – NDIS 2.0, та 32-розрядні варіанти, що використовують розширену пам'ять, – NDIS 3.0, 3.1;*
- ***PDS** (Packet Driver Specification) – компактні пакетні драйвери, розроблені фірмою FTP Software для підтримки Unix-систем та протоколу TCP/IP.*

Функціонально програмі ipx.com для Novell Netware 3.11 в Novell Netware 4.x відповідає комплекс програм. Він складається з таких частин.

• **Драйвер мережевого адаптера** виконаний згідно зі специфікацією ODI. Він дає змогу передавати кадри у форматах різних протоколів. Постачають у вигляді виконавчого файлу, наприклад, 3C5X9.com для адаптера *Etherlink* фірми 3COM та ne200.com для адаптера *NE200* фірми Eagle.

• **Програма керування LSL** (Link Support Layer) фактично реалізує специфікацію ODI та є посередником між програмами драйверів адаптерів і протоколами комунікації мережевого

та транспортного рівнів. LSL дає змогу одному адаптеру обслуговувати кілька протокольних стеків, а кільком платам – один стек.

• **Програми протоколів мережевого та транспортного рівнів**. Ними можуть бути ipxodi.com для протоколу SPX/IPX та tcpip.exe для протоколу TCP/IP.

*Програма ipxodi.com функціонально реалізує опрацювання інформаційних пакетів послідовно протоколами мережевого (**IPX**) та транспортного (**SPX**) рівнів. За допомогою протоколу IPX приєднують до пакетів заголовок з адресною інформацією та передають пакети як данограми (не гарантуючи їх передавання). Протокол SPX поліпшує характеристики IPX, вводячи контроль передавання інформації мережею, перевіряє правильність передавання з використанням контрольних сум, працює з підтвердженнями. Якщо після кількох спроб передати інформацію не вдається, то надходить повідомлення про розірвання сполучення.*

Для початкового запуску робочої станції використовують командний файл DOS startnet.bat. Він містить команди початкового завантаження станції в такій послідовності: lsl, драйвер мережевого адаптера, програма ipxodi.com.

39.4. Структура та головні функції запитувача DOS

Роль оболонки shell в ОС Novell Netware 4.x відіграє окремий комплекс програм, який називають **запитувачем DOS** (DOS requester). Аналогічно до netx він пов'язує прикладну програму та мережеву ОС, виконуючи функції переспрямування.

На відміну від netx, який опрацьовує запити до ресурсів без участі DOS, запитувач працює разом з DOS, одержуючи запити через інтерфейс переадресування DOS (Int 2Fh). DOS визначає, кому адресовано запит, і, якщо потрібно, переспрямовує його до запитувача.

Запитувач DOS має модульну структуру. Головною в ньому є програма **Менеджер vlm**, яку позначають vlm.exe. Вона приймає запити та спрямовує їх для виконання відповідному функціональному модулю vlm, керує пам'яттю, яку використовує модуль vlm, інтерпретує командний файл конфігурації запитувача net.cfg, під час входження у мережу перевіряє наявність серверів та приєднує користувача до конкретного сервера.

Окремі модулі, до яких звертається Менеджер vlm, мають розширення vlm (Virtual Loadable Module). Їх можна розділити на *мультиплексери* (модулі, які керують іншими модулями) та робочі модулі (в англійській термінології child). Кожен робочий модуль підтримує певну логічну функцію. Приклади окремих vlm та їхні призначення наведені у табл. 39.1.

Таблиця 39.1. Модулі vlm

Назва	Призначення
redir	Виконує функції програми переспрямування
nds	Підтримує NDS
pnw	Підтримує одноранговi мережі
rsa	Реалізує алгоритм шифрування для ідентифікації користувача та доступу до функцій керування. Автори алгоритму - Rivest, Shamir, Adleman
bind	Емулює послуги bindery
nwp	Мультиплексер vlm. Керує nds, rsa, bind, pnw
fio	Функції введення-виведення
cache	Обслуговує кеш
print	Керування друкуванням
ipxncp	Служба протоколу IPX
tcpncp	Служба протоколу TCP
tran	Мультиплексер транспортного протоколу
auto	У випадку розірвання сполучення знову сполучає клієнта з сервером
conn	Менеджер сполучень. Охоплює всі рівні архітектури запитувача та дає змогу налагодити задану кількість з серверами за допомогою параметрів з net.cfg
netx	Емулює програми оболонки попередніх версій Netware
tbmi2	Дає змогу протоколу SPX/IPX працювати у багатозадачних середовищах. Реалізує перемикання між задачами

Структурно запитувач DOS поділяють на чотири рівні (рис. 39.3).

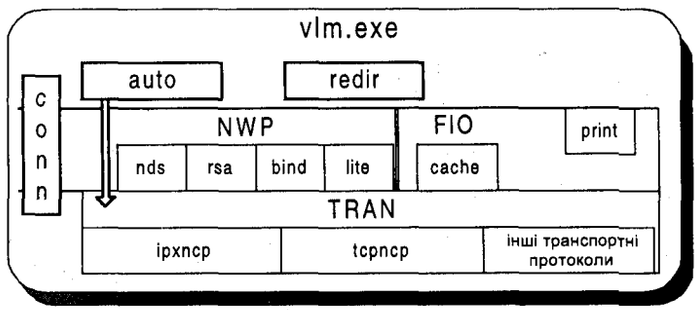


Рис. 39.3. Структурна схема запитувача DOS.

На першому (верхньому) рівні є Менеджер vlm. Під час роботи станції він завжди завантажений та керує модулями vlm. Другий рівень називається рівнем *переспрямування DOS (DOS Redirection Layer)*. Функції переспрямування виконує модуль redir.vlm. Третій рівень – це рівень *сервісних протоколів (Service Protocol Layer)*. Тут є багато модулів. На четвертому рівні, який називають рівнем *транспортного протоколу (Transport Protocol Layer)*, мультиплексор транспортних протоколів tran.vlm керує модулями транспортних протоколів ipxncp та tcpncp.

39.5. Конфігураційний файл net.cfg

Для керування запитувачем DOS є спеціальний конфігураційний файл, що міститься в каталозі nwclient кожної станції. У ранніх версіях Netware цей файл називався shell.cfg, а в Novell Netware 4.x – net.cfg. Це текстовий командний файл, що може містити такі чотири розділи:

• [Link driver] визначається драйвер мережевого адаптера та його параметри; наприклад, ця секція конфігураційного файлу може мати вигляд

```
[Link driver]
3C5X9
Port 300
Int 10
Frame Ethernet 802_2
```

• [Link support] визначаються ємність буферів для проміжного зберігання інформації, кількість адаптерних плат та стеків;

• [Protocol] задається підтримка різних протоколів; конфігурація параметрів програм протоколів NETBIOS, ipxodi;

• [Netware Dos Requester] задаються параметри конфігурації робочої станції.

Найпотрібнішими є такі команди:

auto reconnect on/off; якщо задано режим on, то auto.vlm у разі порушення сполучення спробує знову приєднати клієнта до сервера. Якщо задано off, то приєднання виконує користувач;

name context=<контекст> задати контекст, який задається кожного разу під час завантаження станції;

preferred server=<назва серверного об'єкта> задати ім'я серверного об'єкта, до якого станція буде приєднуватись під час завантаження;

preferred tree=<назва дерева>.

39.6. Особливості програмного забезпечення робочої станції

Додатковими особливостями програмного забезпечення, що реалізовані на рівні робочої станції, є використання *протоколу багатопакетного передавання (Packet Burst Protocol)*, *протоколу великих міжмережевих пакетів (Large Internet Packets)* та *механізму електронного підписування пакетів.*

Протокол багатопакетного передавання (ПБП) призначений для передавання пачки пакетів міжмережевим з'єднанням з підтвердження пачки як одного цілого. Для використання цього протоколу потрібно додаткові буфери пам'яті, однак це значно пришвидшує передавання завдяки зменшенню інформації перевіряння. У разі завантаження станції вона та сервер узгод-

жують між собою розмір пачки пакетів. Згодом, у випадку передавання більше одного пакета використовується ПБП, що діє за замовчуванням. Відімкнути його можна, якщо в net.cfg у секції [Netware DOS Requester] записати

PB BUFFERS=0.

Протокол великих міжмережевих пакетів дає змогу передавати через мости та маршрутизатори великі пакети. У ранніх версіях Novell Netware розмір пакета, який проходив через маршрутизатор, не міг перевищувати 576 байт. Під час налагодження сполучення робоча станція узгоджувала максимальний розмір пакета з сервером, який перевіряв, чи є на шляху пакетів між ним та робочою станцією маршрутизатор. Якщо маршрутизатор був, то максимальний розмір пакета дорівнював 576 байт. У Novell 4.x таких обмежень немає, що дає змогу збільшити швидкість передавання інформації через маршрутизатори.

Механізм електронного підписування пакетів діє як одна з компонент загальної системи безпеки. У випадку вмикання цього режиму кожен пакет підписує сервер або робоча станція. Підпис перевіряється під час одержання. Якщо підпис неправильний, пакет ігнорують і про факт його появи повідомляють робочу станцію і сервер. Підписи різні на кожному пакеті. Використання механізму електронного підписування пакетів практично не дає змоги зловмиснику замінити пакети. Рівень захисту задають окремо для станції та сервера числом від 0 (електронного підпису і захисту немає) до 3 (найбільші вимоги до захисту). За замовчуванням є рівень захисту 1. Для задання рівня захисту на станції в net.cfg записують команду

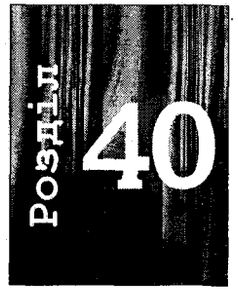
signature level=<рівень захисту> .

Детальніша інформація про механізм електронних підписів є в розділі 41.

Бібліографія та джерела

Ценк А. Novell Netware 4.x. К.: BHV, 1996.

ФАЙЛОВА СИСТЕМА ОС NOVELL NETWARE 4.x



Структура та загальна характеристика файлової системи. Том. Том як об'єкт NDS. Внутрішня організація тому. Робота з томом. Використання файлів різних операційних систем. Міграція та стиснення даних. Організація роботи HCSS. Каталоги. Системні каталоги сервера. Планування структури каталогів. Файл як елемент файлової системи. Системні файли. Атрибути файлів. Права доступу до файлів. Операції над файлами.

Як зазначено, операційна система Nowell Netware 4.x складається з двох частин: NDS та файлової системи. У цьому розділі ми розглянемо другу складову частину ОС – **файлову систему (ФС)**.

40.1. Структура та загальна характеристика файлової системи

Файлова система Novell Netware 4.x має ієрархічну структуру (рис. 40.1). Головними елементами такої структури є томи, каталоги, підкаталоги та файли. Окрім цих елементів, для роботи з файловою системою використовують і деякі об'єкти NDS.

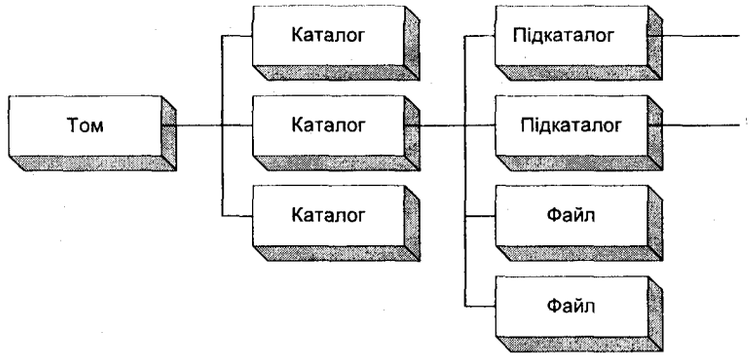


Рис. 40.1. Структура файлової системи.

Головний елемент ФС – том. Томи створюють під час інсталювання операційної системи і розміщують на серверах. На одному сервері може бути до 64 томів. Максимальний розмір тому – 32 Тбайт. Максимальна кількість файлів тому – 2097152.

Каталоги та підкаталоги є наступними в ієрархії об'єктами організації даних у ФС. Кількість каталогів та вкладених підкаталогів обмежена тільки наявним дисковим простором.

Файл – це найнижча структурна одиниця файлової системи Novell Netware 4.x. Він має ім'я та атрибути, що характеризують операції, які можна з ним виконувати.

40.2. Том

Том – це певна фіксована частина розділу Netware на твердому диску. Томи створюють під час інсталювання системи. Цікавою особливістю тому є те, що йому одночасно відповідають як об'єкт NDS, так і том ФС. Отже, том – це та ланка, яка об'єднує NDS та ФС.

Том як об'єкт NDS. Конфігурування тому під час інсталювання

Об'єкт NDS, що відповідає тому, має ім'я

<ім'я сервера>_<ім'я тому>

Наприклад: icm_server_sys, server1_sys, server2_vol1. На кожному сервері обов'язково є системний том з ім'ям sys.

У властивостях цього об'єкта відображені імена сервера та відповідного тому ФС, тут також є статистична інформація про том: розмір блоку, задані риси, час створення, час останнього запису, розмір у кілобайтах, використаний та вільний простір.

Під час налаштування на рівні тому можна задати або відмінити два режими його функціонування: стиснення інформації та раціональне використання блоків (див. розділ 37).

Стиснення інформації на рівні тому передбачає режим стиснення файлів за замовчуванням. Це дає змогу дозволяти або забороняти стискування інформації для окремих файлів.

Режим **додаткового використання блоків** дає змогу економніше використовувати дисковий простір. Кожен частково використаний блок розділяється на частини по 512 байт. Незайняті частини можуть бути зайняті іншими файлами. Інформація про використання таких блоків є в спеціальних системних зведеннях – таблицях додаткового використання блоків. Приклад: нехай блок на сервері має розмір 4096 байт, а файл x.dat – 4200 байт. Якщо режим додаткового використання блоків вимкнутий, то файл буде займати на сервері два блоки – 8192 байт, в іншому разі – 4096+512=4608 байт. У цьому випадку будуть використані один блок повністю та одна восьма частина іншого блоку. Наступний файл буде записуватися у вільне місце іншого блоку. Використання цього режиму потребує додаткового збереження та опрацювання інформації про використання блоків, а це відповідно, додаткових витрат ресурсів комп'ютера.

Оскільки кожному тому відповідає об'єкт NDS типу *том*, на цей об'єкт для будь-якого іншого об'єкта NDS можна задати права доступу, наприклад, зробити том 'невидимим' чи обмежити доступ тільки читанням для якогось користувача або групи користувачів.

Внутрішня організація тому

Кожен том поділяють на частини двома способами:

• **логічно** – томи поділяють на каталоги, підкаталоги, файли; виконують адміністратор або користувачі системи, які мають на це право;

• **фізично** – том поділяють на сегменти. Кожен том може складатися з різної кількості сегментів – від 1 до 32, причому на одному твердому диску може бути до 8 сегментів.

Поділ тому на сегменти дає змогу розташувати його на різних твердих дисках, зокрема на різних дисках – різні сегменти одного тому. Операції записування та читання файлів такого тому відбуваються одночасно на двох дисках, що значно пришвидшує процес. З іншого боку, у разі виходу з ладу одного з твердих дисків недоступними стають усі томи, хоча б один сегмент яких був на цьому диску.

Отже, том можна розмістити на одному диску або на кількох, або ж на одному диску розмістити кілька томів.

Як зазначено, томи створюють під час налаштування системи. Нові томи можна додати згодом, приєднавши нові тверді диски. Так само можна додати нові сегменти до вже наявних томів. Нові томи та сегменти створюють утилітою install.

Найменшою одиницею дискового простору, що адресується в томі, є блок. Усі блоки тому мають однаковий розмір, який задають під час інсталювання. Як звичайно, чим більша ємність твердого диска, тим розмір блоку більший. За замовчуванням розміри блоку змінюються від 4 до 64 Кб. Чим менший блок, тим більше місця в пам'яті займає інформація керування тому і тим довше виконуються операції над файлами. З іншого боку, чим більший блок, тим менш ефективно використовується дисковий простір. Під час налаштування системи користувач може сам вибрати розмір блоку, оскільки згодом його змінити вже не можна.

Для керування роботою тому в деяких його блоках зберігаються таблиці керування *DET* та *FAT*.

DET (Directory Entry Table) – це таблиця записів про каталоги та файли. Вона містить інформацію про підкаталоги, файли тому, довірених осіб та їхні права. Кожен запис таблиці (про файли та каталоги) має такі поля:

• назва каталогу або файлу,
• власник,
• дата останньої модифікації (для файлів),
• місце розташування першого блоку каталогу або файлу.

DET використовують для шукання файлу. Кожен запис DET займає 32 байти. Для збереження DET виділяють блоки, які називають *блоками каталогу*. Якщо блок займає 4096 байт, то максимальна кількість записів – 128. Том sys початково має сім блоків каталогу. Згодом, якщо потрібно, можна додати нові. Інформація DET кешується. Максимальна кількість блоків каталогів на том – 65536. Отже, максимальна кількість записів у DET, яка дорівнює максимальній кількості файлів у томі, – 2097152.

FAT (File Allocation Table) – це індексна таблиця розміщення файлів, яку використовують для об'єдання файлів з окремих блоків. Доступ у FAT відбувається через DET. FAT також кешується у пам'яті. Кожен том має свій FAT. Записи у FAT відповідають номерам блоків файлу. У цьому робота FAT Novell Netware 4.x аналогічна до роботи FAT-таблиць DOS.

Якщо розмір файлу перевищує 64 блоки, то для прискорення доступу до нього будують індекс FAT – *Turbo FAT*. Елементи цього індексу послідовно містять номери комірок FAT-таблиці, де зберігається інформація про розміщення файлу.

З метою прискорити операції вибирання та записування інформації значну частину оперативної пам'яті сервера використовують як кеш-пам'ять, оскільки читання або записування інформації з пам'яті відбуваються у сотні разів швидше, ніж з твердого диска. У кеш-пам'яті зберігають найважливіші системні таблиці: геш-таблиці, FAT, Turbo FAT, таблиці додаткового використання блоків, каталоговий кеш. Є також тимчасовий простір збереження для файлів та модулів nml. Файли, які використовують менше, вилучаються з кешу першими (рис. 40.2).

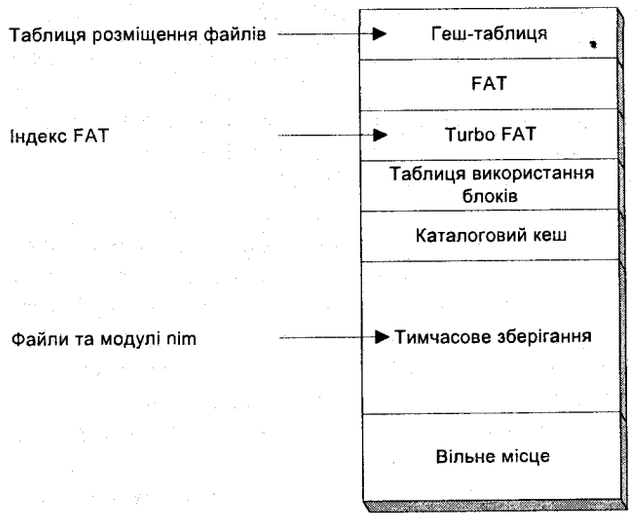


Рис. 40.2. Використання кеш-пам'яті.

Робота з томом

Монтування та демонтування. Як відомо, змонтувати том – це зробити його інформацію доступною для користувачів. Кожного разу під час завантаження системи відбувається монтування деяких томів. Інформація про кожен том (геш-таблиця, FAT, Turbo FAT, каталоговий кеш та ін.) зберігається в пам'яті окремо. Для економії пам'яті та зменшення тривалості опрацювання таблиць доцільно томи, які використовують зрідка, монтувати тільки у разі потреби. Демонтування – процес, обернений до монтування. Під час демонтування закриваються та стають недоступними всі файли тому, який демонтують.

Створення, знищення, перейменування, змінювання параметрів. Усі головні операції з томами виконують за допомогою утиліти install. Системний том створюється під час інсталювання сервера. Тоді ж формується відповідний об'єкт NDS у контексті серверного об'єкта. Згодом, якщо треба, об'єкт тому можна перемістити в інший контекст.

Якщо на сервері з'являється додатковий дисковий простір (унаслідок знищення якогось тому або встановлення нового твердого диска), користувач може збільшити розмір наявних томів у мережі або створити новий том. Збільшити розмір наявного тому можна, додавши до нього новий сегмент та визначивши його розмір. Коли сегмент є новим (тобто на нього ще не записували інформації), його розмір можна змінювати довільно. Змінити розмір наявного сегмента неможливо. Новий сегмент можна додати до довільного тому на будь-якому сервері з урахуванням обмежень на кількість сегментів у томі та на сервері.

Знищують том або його сегмент за допомогою утиліти install (розділ *Maintenance/Selective install – Обслуговування/Часткове інсталювання*), попередньо демонтувавши їх. У цьому випадку зникає вся інформація тому і дисковий простір, який він займав, стає вільним.

Перейменовують том або змінюють його параметри також утилітою install. Для цього ім'я відповідного об'єкта NDS треба змінити окремо засобами адміністрування NDS. Не можна змінити ім'я системного тому sys.

Перевірка та ремонт таблиць керування. Кожного разу під час монтування тому система перевіряє цілісність структур керування тому. Тільки том, таблиці керування якого правильні, можна змонтувати. Якщо виявлені порушення структури, про це надходить повідомлення і запускається утиліта ремонту тому vrepair. Цю утиліту можна запустити і для будь-якого незмонтованого тому, якщо змонтовані інші томи. Порушення структури таблиць може бути спричинене вимкненням живлення сервера, помилками читання з твердого диска, незбіжністю змісту копій FAT- та DET-таблиць (для більшої надійності система зберігає дві копії FAT- та DET-таблиць).

Використання файлів інших операційних систем. Операційна система Novell Netware 4.x дає змогу зберігати та використовувати на одному томі файли інших ОС (Unix, Apple Macintosh, OS/2) і працювати з ними з робочих станцій у відповідних системах. Для цього треба *попередньо завантажити у пам'ять блок простору імен (name space)*, що відповідає потрібній операційній системі. Блоки простору імен оформлені як завантажувальні модулі Netware (вони мають розширення nam), їх завантажують з консолі сервера або в командному файлі завантаження сервера командою

load <name_space>.nam.

Потім пов'язують том з блоком простору імен командою

add name space <name_space> to <volume_name>.

Після цього у томі поряд з файлами DOS зможуть зберігатися файли інших операційних систем.

У випадку додавання нового простору імен вимоги до пам'яті збільшуються майже удвічі. Тобто для кожного недосівського файлу в таблиці записів про каталоги та файли зберігаються два записи: один подає файл як DOS-файл, інший – як файл іншої операційної системи. Наприклад, якщо до диска додано простір імен для файлів Macintosh, то кожен Mac-файл має в таблиці каталогів два записи (рис. 40.3).

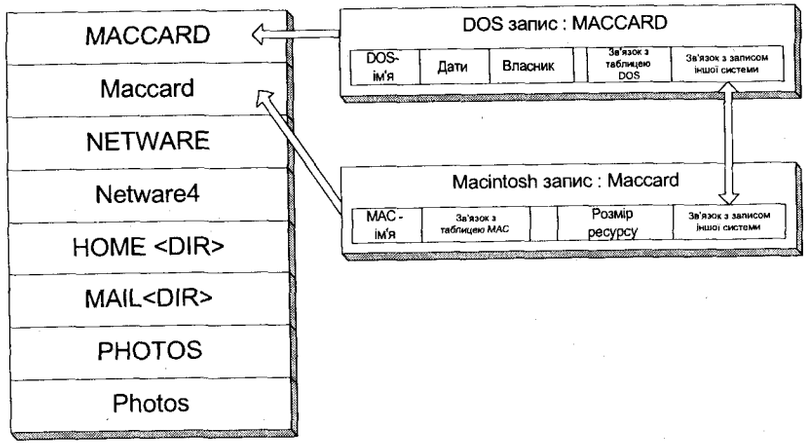


Рис. 40.3. Структура таблиці каталогів у випадку використання простору імен Mac.

Точніше потрібну ємність пам'яті для завантаження нового простору імен можна обчислити за формулою

0.032 (розмір тому, Мб)/(розмір блоку, Кб).

Результат заокруглюють до найближчого більшого мегабайта. Якщо пам'яті для нового простору імен не вистачає, том не монтується.

Зазначимо таке: якщо до тому додано новий простір імен, то зняти його можна тільки за допомогою утиліти vrepair *або знищивши том взагалі. Якщо том має інстальований простір імен, то, перш ніж монтувати його, треба завантажити в пам'ять відповідний пат-файл та прив'язати його до тому. Без цього том не монтуватиметься.*

Міграція даних. На рівні тому з використанням утиліти install.nlm можна дозволити або заборонити режим *міграції даних*. Якщо міграція даних дозволена, система простежує частоту використання окремих каталогів та файлів і ті з них, які використовуються зрідка, автоматично переносить на зовнішні носії інформації (магнітні стрічки, оптичні диски тощо). Унаслідок цього звільняється місце на твердому диску сервера. Для користувача системи ці файли виглядають так, як і на твердому диску сервера, і доступ до них такий самий, тільки з більшою затримкою, що зумовлено читанням із зовнішнього носія. Детальніша інформація про систему міграції даних у Novell Netware 4.x наведена в Д.40.1.

Стиснення даних. Стиснення даних – це альтернатива використанню міграції даних.

40.3. Каталог

Як відомо, каталог – це наступний після тому елемент структурної організації ФС. Каталоги дають змогу згрупувати файли за певними ознаками та визначити права доступу до груп файлів.

Системні каталоги

Під час налаштування операційної системи створюють такі каталоги.

• deleted.sav містить усі файли, вилучені з диска, до їх знищення. Файли з каталогу deleted.sav можна поновити.

• etc містить зразки програм конфігурації сервера, зокрема для роботи з Unix-станцією за допомогою протоколу TCP/IP.

• login містить файли, потрібні користувачу для реєстрування в системі (такі як login.exe). Каталог може містити підкаталог з програмами реєстрації користувачів OS/2 та каталог nls з системними повідомленнями.

• public містить загальнодоступні утиліти для керування системою. Подібно до каталогу login, тут може бути підкаталог з утилітами OS/2 та каталог системних повідомлень утиліт nls.

• system містить файли операційної системи та утиліти адміністратора мережі. Має підкаталог nls для системних повідомлень.

• mail використовують для сумісності з попередніми версіями Netware. Якщо удосконалюють стару версію Netware, то в цьому каталозі будуть підкаталоги індивідуально для кожного з користувачів, де міститимуться командні файли (login scripts) цих користувачів.

• dos – це каталог для файлів електронного підручника Novell Netware 4.x (*Novell Electrotext*).

Атрибути каталогів

Кожен каталог, як і файл, має свій запис у таблиці каталогів, де відображені ім'я каталогу, його власник, адреса на диску (початок ланцюжка FAT), атрибути, дата створення та інша інформація. **Атрибути каталогу** – це властивості, які стосуються всіх файлів каталогу і чинні для всіх користувачів без винятку. Наприклад, якщо для каталогу задано атрибут DI, то ніхто, навіть адміністратор системи, не зможе знищити файл, попередньо не змінивши атрибут. Список можливих атрибутів та їхні пояснення наведено в табл. 40.1.

Таблиця 40.1. Атрибути каталогів

	Назва атрибуту		Примітка
Dl	Delete Inhibit	Заборонити знищення	Каталог не можна знищити
Dc	Don't compress	Заборонити стиснення	Файли каталогу не можна стиснути
Dm	Don't migrate	Заборонити міграцію даних	Заборонено міграцію даних каталогу на зовнішні носії даних (HCSS)
H	Hidden	Схований	Атрибут систем MSDOS та OS/2. Такий каталог не відображатимуть команди dir цих ОС. Його не можна знищити або перейменувати. Проте каталог можна буде відобразити командою ndir, якщо користувач має на цей каталог право FileScan
Ic	Immediate compress	Стиснення без затримки	Операційна система стискає файли каталогу, якщо трапиться будь-яка нагода, не очікуючи на певну подію (наприклад, закінчення тайм-ауту)
N	Normal	Нормальний режим	Каталог не має жодних атрибутів
P	Purge	Очищення	Задає режим очищення для всіх файлів каталогу незалежно від їхніх атрибутів. Якщо файл знищено, він відразу вилучається з диска без можливості поновлення
Ri	Rename Inhibit	Заборонити перейменування	Заборонено перейменовувати каталог
Sy	System	Системний	Атрибут систем MSDOS та OS/2. Такий системний каталог не відображатимуть команди dir цих ОС. Його не можна буде знищити або перейменувати. Проте каталог можна буде відобразити командою ndir, якщо користувач має на цей каталог право FileScan

Права доступу до каталогів. Мати доступ до каталогів, тобто бути зареєстрованими як довірені особи каталогу, можуть такі типи об'єктів NDS:

- користувач – User;
- група користувачів – Group;
- посада – Organizational Role.

Для кожного такого об'єкта можна визначити набір прав. Повний набір прав на каталог наведено в табл. 40.2. Права на каталог задають утилітами nwadmin та filer. Якщо для довіреної особи задано право на якийсь каталог, його успадковують усі вкладені каталоги. Успадкування можна блокувати за допомогою фільтрів успадкованих прав (IRF) аналогічно до об'єктів NDS.

Операції над каталогами

Прості операції над каталогами – це *створення*, *перейменування*, *знищення* каталогу, а також його *відображення*.

Створення, перейменування, копіювання, перенесення каталогів. Операції створення, перейменування, копіювання, перенесення та знищення каталогу виконує користувач з відповідним набором прав за допомогою утиліт nwadmin та filer.

Таблиця 40.2. Права на каталог

	Назва права		Примітка
S	Supervisor	Право адміністратора	Дає всі права на каталог, його підкаталоги та файли. Його не можна блокувати фільтром успадкованих прав. Користувач з таким правом може надавати іншим користувачам права на цей каталог його підкаталоги та файли
R	Read	Читання	Дає право відкривати, переглядати та виконувати файли в каталозі
W	Write	Записування	Дає змогу відкривати та змінювати зміст файлів у каталозі
C	Create	Створення	Дає змогу створювати нові підкаталоги та файли в цьому каталозі. Якщо користувач не має інших прав, крім C, він може створити новий підкаталог або файл. Однак у разі закриття такого файлу відкрити його зможе тільки користувач з більшим набором прав
E	Erase	Вилучення	Дає змогу вилучати в цьому каталозі файли або інші підкаталоги
M	Modify	Змінювання	Дає змогу змінювати атрибути назви файлів та підкаталогів каталогу, але не їхній зміст
F	File Scan	Переглядання	Дає змогу бачити файли та підкаталоги каталогу за допомогою команд ndir та dir
A	Access control	Контроль доступу	Дає право змінювати і призначати права та фільтри успадкованих прав для інших довірених осіб на цей каталог, його підкаталоги та файли

Операція знищення каталогу. Процес знищення (delete) каталогу (як і файлу) має дві стадії. Вилучати, поновлювати та знищувати каталоги можуть тільки користувачі з адміністративними правами на ці каталоги. На першій стадії каталог *вилучається*, а інформація з нього надходить у системний каталог deleted.sav, звідки її можна поновити або знищити. Якщо каталог не поновлюють протягом деякого заданого часу, він знищується (purge) з системного каталогу deleted.sav і поновити його не можна. Вилучені каталоги знищуються й автоматично, якщо на диску сервера не вистачає місця для записування.

Відображення каталогу (drive mapping). Під час роботи з каталогами в DOS виділяються операції відображення каталогу. Для доступу до каталогу використовують такий запис:

{<сервер>}\<том>:<каталог>[{\<підкаталог>}...[\<підкаталог>]].

Наприклад:

```
sys:texty
serv1\vol1:msdoc\texty
```

Поле з іменем сервера є необов'язковим, його застосовують для шукання сервера в іншому контексті. З метою спростити звертання до каталогу цей каталог відображають на певний логічний диск за допомогою команди відображення map. Наприклад:

```
map k:=serv1\vol1:proekt\buch.
```

Після цього до каталогу можна звертатися за позначенням логічого диска k:

```
k:\nakl.txt.
```

Максимально можна перевизначити до 32 логічних дисків.

Окрім простого закріплення за конкретними каталогами позначень логічних дисків, у Novell Netware 4.x, як і в попередніх версіях ОС Novell Netware, можна визначити **розшукові вказівники** (search drives). Значення цих вказівників еквівалентне заданню маршрутів шукання командою DOS path.

Якщо потрібного файлу в активному каталозі нема, його шукатимуть у каталогах, на які задано розшукові вказівники.

Кожен розшуковий вказівник позначають буквою *s* з номером (від 1 до 16). Під час роботи системи кожному розшуковому вказівнику буде присвоєно логічний диск, починаючи з z для s1 і далі вгору за алфавітом. Для присвоєння розшукового вказівника використовують команду відображення map. Наприклад:

map s1:=vol2:guest\carol.

Вказівник s16 дає змогу присвоїти кільком каталогам наступні невикористані позначення логічних дисків, не змінюючи позначень попередьо призначених, а також закріпити за конкретним розшуковим вказівником конкретний логічний диск. Для цього використовують команду map такого вигляду:

map s16:=<логічний диск>=<каталог>.

Кожна робоча станція може використовувати логічні диски від a до z. Як звичайно, диски a, b – це локальні дисководи гнучких дисків, c, d, e відповідають локальному твердому диску, починаючи з f – мережеві логічні диски, а в кінці алфавіту (x, y, z) – розшукові вказівники.

Використання об'єкта *відображення каталогу* (Drive mapping). Зручно керувати файловою системою дають змогу об'єкти NDS типу *відображення каталогу*. Цей об'єкт відповідає конкретному каталогу. Об'єкти типу *відображення каталогу* можуть бути у команді відображення map. Наприклад:

map j:=cn=dos.ou=ism.ou=fkt.o=techn_univ.

Логічному диску j відповідатиме каталог, закріплений за об'єктом

cn=dos.ou=ism.ou=fkt.o=techn_univ.

Переваги використання об'єкта типу *відображення каталогу* такі. Наприклад, на робочій станції є операційна система DOS 5.0, що зберігається у каталозі DOS50. Цей каталог неодноразово згаданий у різних командах різних командних файлів налагодження системи. Користувачу треба змінити операційну систему на DOS 6.22. Для цього він створив каталог DOS622 та записав у нього відповідні файли. Тепер для конфігурування системи в користувача є два шляхи.

• Якщо немає об'єкта типу *відображення каталогу*, що відповідає каталогу DOS50, користувач повинен у всіх командних файлах змінити посилання DOS50 на DOS622. Цей процес може тривати довго і бути джерелом помилок та збоїв під час роботи системи.

• Якщо ж об'єкт типу *відображення каталогу*, що відповідає каталогу DOS50, є, то користувачу достатньо один раз у цьому об'єкті змінити DOS50 на DOS622.

Спеціальні каталоги

• **Каталоги з операційною системою робочих станцій.** Якщо в системі використовують бездискові робочі станції або треба зекономити місце на локальних твердих дисках, у Novell Netware 4.x можна завантажувати станції з сервера. У цьому випадку на сервері створюють каталоги з відповідними операційними системами (якщо вони різні).

• **Каталоги HCSS.** На кожному сервері в одному з томів можна створити один або кілька каталогів *HCSS (High Capacity Storage System) – систем зберігання великої ємності*. У цих каталогах реалізовано режим міграції даних на зовнішні носії – батарею оптичних дисків, або стример. Детальніше про систему HCSS див. Д.40.1.

Планування структури каталогів. Перш ніж розпочати роботу, потрібно ретельно спланувати структуру файлової системи, оскільки правильно сплановану систему каталогів просто обслуговувати. У цьому випадку можна керуватися такими правилами.

• Для прикладних програм створюють окремі каталоги. Це дає змогу не архівувати файли прикладних програм зайвий раз (якщо є дистрибутиви).

• Для файлів даних створюють окремі каталоги. Це полегшує їх періодичне архівування.

• Кожен користувач повинен мати окремий каталог для зберігання своїх файлів з обмеженим правом доступу до нього інших користувачів.

• Файли спільного використання робочої групи можна зберігати в окремому каталозі робочої групи.

• Можна створити каталоги для зберігання конфігураційних програм роботи з Windows та іншими аналогічними програмами.

• Окремі каталоги створюють для таких загальнодоступних даних, як електронна пошта.

40.4. Файл

Файл – це найменша та головна структурна одиниця ФС.

Системні файли. Системні файли сервера мають такі типи і розширення:

• **nlm** (netware loadable module) – завантажувальний модуль Netware; такими файлами є всі утиліти сервера;

• **nam** (name address module) – використовують для завантаження додаткового простору імен з метою використання файлів різних операційних систем;

• **lan** (local area network) – драйвери адаптерів локальної мережі;

• **dsk** (disk) – драйвери твердого диска.

Атрибути файлу. Кожен файл, як і каталог, може мати набір атрибутів, які характеризують його тип та операції, які з ним можна виконувати. Атрибути файлу стосуються всіх без винятку користувачів файлу. Головні атрибути наведені в табл. 40.3.

Таблиця 40.3. Атрибути файлів

	Назва атрибуту		Примітка
A	Archive Needed	Потрібно зархівувати	Інформує, що файл змінився після останнього архівування. Програми архівування звичайно занулюють цей атрибут
CC	Can't compress	Не можна стиснути	Файл не варто стискувати, оскільки економія місця буде незначною. Атрибут задає система
Co	Compressed	Стиснутий файл	Файл стиснено. Атрибут задає система
Ci	Copy Inhibit	Заборонено копіювати файл	Файл копіювати заборонено. Атрибут діє тільки на станціях Macintosh
Di	Delete Inhibit	Заборонено знищувати файл	Файл не можна знищити
Dc	Don't compress	Не стискувати	Файл не стискується
Dm	Don't migrate	Не переносити на зовнішні носії	Файл не переноситься на зовнішній носій даних
X	Execute only	Тільки для виконання	Файл не можна копіювати. Атрибут задає адміністратор, його не можна занулити. Атрибут задають, якщо в запасі є копія цього файлу
H	Hidden	Схований	Атрибут систем MSDOS та OS/2. Такий файл не відображатимуть команди DIR цих ОС. Його не можна знищити або перейменувати. Проте файл можна відобразити командою ndir, якщо користувач має на цей файл право FileScan
Ic	Immediate compress	Першочергове стиснення	Файл стискується, якщо трапиться будь-яка нагода
I	Indexed	Індексований	Інформує, що розмір файлу перевищив деяке значення і система прийняла рішення про індексування його записів у FAT, щоб зменшити тривалість доступу до інформації. Атрибут задає система
M	Migrated	Файл перенесений на зовнішній носій	Інформує, що файл перебуває в режимі міграції. Атрибут задає система
N	Normal	Номальний режим	Інформує, що жодних атрибутів не задано
P	Purge	Знищити файл	У разі вилучення файл знищується, і його не можна поновити
Ro	Read only	Тільки для читання	Забороняє записування у файл. У випадку задання цього атрибуту автоматично задаються атрибути Di та R, так що файл не можна вилучати або перейменовувати. Користувач, який має право Modify, може відмінити права Di та R, зберігши атрибут Ro
R	Rename inhibit	Заборонити перейменування	Заборонено перейменовувати файл
S	Shareable	Файл спільного використання	Файл можуть колективно використовувати декілька програм одночасно. Звичайно цей атрибут використовують разом з атрибутом Ro
Sy	System	Системний	Атрибут систем MSDOS та OS/2. Такий системний каталог не відображатимуть команди DIR цих ОС. Його не можна знищити або перейменувати. Проте каталог можна відобразити командою ndir, якщо користувач має на цей каталог право FileScan
T	Transactional	Файл в транзакції	Інформує, що файл перебуває під захистом системи простежування транзакцій, яка гарантує, що у разі змінювання файлу або всі зміни відбулися успішно, або жодних змін не було

Таблиця 40. 4. Права на файл

	Назва права		Примітка
S	Supervisor	Право адміністратора	Дає всі права на каталог, його підкаталоги та файли. Його не можна блокувати фільтром успадкованих прав. Користувач з таким правом може надавати іншим користувачам права на цей файл, а також задавати фільтри успадкованих прав
R	Read	Читання	Дає право відкривати та переглядати файли
W	Write	Записування	Дає змогу відкривати та записувати дані в наявний файл
C	Create	Створення	Дає змогу поновити файл після вилучення
E	Erase	Вилучення	Дає змогу вилучити файл
M	Modify	Змінювання	Дає змогу змінювати атрибути файлу та його назву, але не зміст
F	File Scan	Переглядання	Дає змогу бачити файл за допомогою команд ndir та dir
A	Access control	Контроль доступу	Дає право змінювати та призначати права і фільтри успадкованих прав для інших довірених осіб на цей файл

Права доступу до файлів. Мати доступ до файлів, тобто бути зареєстрованими як довірені особи файлу, можуть такі типи об'єктів NDS:

- користувач – User;
- група користувачів – Group;
- посада – Organizational Role.

Для кожного такого об'єкта можна визначити набір прав. Права на каталоги і файли є різними. Повний набір прав на файл наведено в табл. 40.4. Права на файл задають утилітами nwadmin та filer. Ефективні права кожного користувача на файл формують як комбінацію його особистих, посадових та групових прав на цей файл з урахуванням атрибутів файлу, прав користувача на каталог, де розташований файл, та атрибутів цього каталогу.

Операції над файлами. Головні операції над файлами – створення, перейменування, копіювання та перенесення, знищення, задання атрибутів, прав доступу. Їх виконують засобами утиліт filer або nwadmin. Деякі особливості має керування стисненням файлу.

Стиснення файлів дає змогу зекономити місце на твердому диску. Якщо стиснення дозволене на рівні тому та каталогу, то для файлу в його атрибуті можна дозволити або заборонити стиснення. За замовчуванням, якщо стиснення дозволене, система аналізує час останнього використання файлу, і, якщо файл не використовували протягом заданого проміжку часу, стискує його. У випадку звертання до такого файлу він розархівовується. Проміжок часу задає адміністратор засобами адміністрування.

Бібліографія та джерела

Ценк А. Novell Netware 4.x. К.: BHV, 1996.

ДОДАТОК ДО РОЗДІЛУ 40

Д. 40.1. Міграція даних та керування нею

Міграція даних – це ефективний спосіб збереження великих обсягів даних з використанням зовнішніх носіїв інформації – оптичних дисків або магнітних стрічок. Найчастіше з цією метою використовують оптичні диски читання/записування (rewritable). Пристроєм, який виконує записування та читання з оптичних дисків, є так званий *Jukebox*. Так називали старовинний автомат для програвання грамплатівок. Цей автомат за запитом користувача вибирав з групи грамплатівок потрібну, передавав її зі сховища у пристрій читання і вмикав музику. Аналогічно, пристрій для роботи з бібліотекою оптичних дисків за запитом вибирає зі сховища потрібний оптичний диск, переміщає його в *Jukebox* і виконує операції читання або записування

HCSS використовує вільний простір на твердому диску для тимчасового кешування найактивніших файлів. Менш активні файли потрапляють на оптичний диск. Цей процес називається **міграцією**. (Отже, міграцію теж можна вважати кешуванням між швидким твердим та повільним оптичним дисками). Якщо користувач домагається доступу до файлу, що зберігається на оптичному диску, система переписує файл з оптичного на твердий диск. Цей процес називається **деміграцією** (рис. Д.40.1.1).

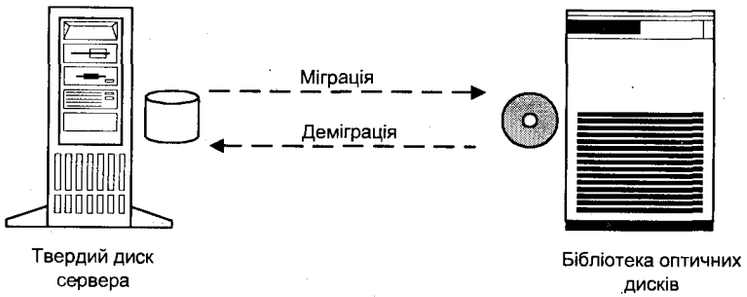


Рис. Д.40.1.1. Міграція та деміграція даних.

Для доступу до даних на оптичних дисках використовують ті ж команди оперативної системи, що й для доступу до даних на твердому диску. З погляду користувача каталоги та файли на оптичному диску нічим не відрізняються від каталогів та файлів на твердому диску.

Рішення про міграцію файлу приймають на підставі даних про ступінь використання твердого диска, тобто про межу використання (*capacity threshold*) та дати останнього використання файлу. Межа використання – це відсоток від ємності твердого диска, на який його можна заповнити до того, як файли почнуть мігрувати. Цей параметр задають та змінюють засобами адміністрування системи.

Міграція даних – це альтернатива іншим засобам ефективного збереження даних: стисненню даних та додатковому використанню блоків. Тому для кожного тому можна використовувати або стиснення та (необов'язково) додаткове використання блоків, або міграцію даних. На кожному сервері може бути тільки один том з міграцією даних. Її задають під час налаштування операційної системи (не можна змінити для тому пізніше).

У томі, в якому дозволено HCSS, адміністратор може створити кілька кореневих каталогів HCSS. Кожному боку кожного оптичного диска присвоюють унікальну позначку, яка згодом є назвою підкаталогу першого рівня. Ємність одного боку оптичного диска, і, відповідно, ємність одного каталогу першого рівня становить близько 500 Мб. Схема організації зберігання даних на оптичних дисках показана на рис. Д.40.1.2.

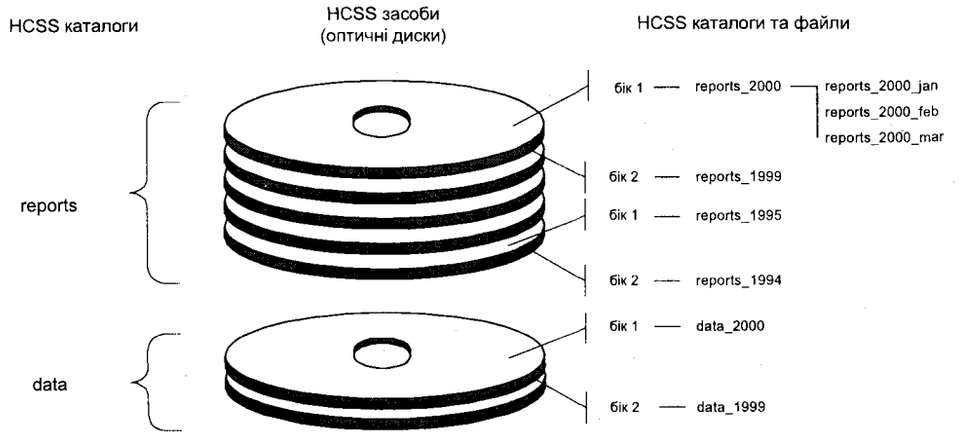


Рис. Д.40.1.2. Схема організації зберігання даних HCSS.

Організація та керування каталогами HCSS відрізняються від керування звичайними каталогами. Тому в назвах кореневих каталогів та каталогів першого рівня HCSS доцільно відобразити факт належності їх до HCSS.

Кореневими каталогами HCSS керують за допомогою засобів адміністрування мережею і спеціальних команд. Спроба використати для цього команди керування звичайними каталогами може призвести до порушення структури файлової системи. З каталогами нижчих рівнів можна працювати як зі звичайними каталогами ФС.

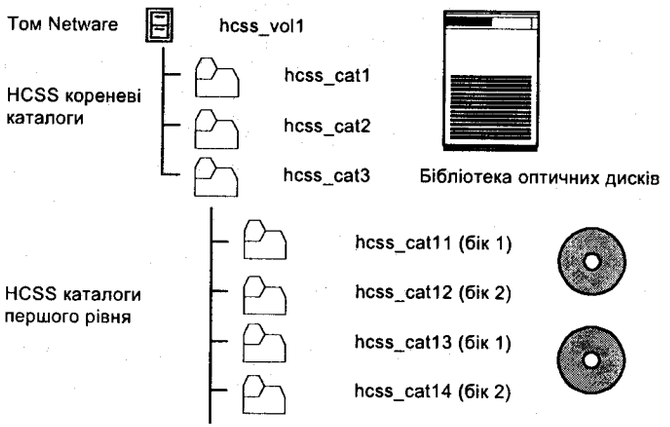


Рис. Д.40.1.3. Структурна організація каталогів HCSS.

Користувач може мати доступ і виконувати операції з каталогами HCSS так само, як зі звичайними каталогами, за винятком того, що підкаталоги, які відповідають бокам оптичного диска, не можна витерти. Так само їм присвоюють і права доступу. Приклад структури каталогу HCSS зображено на рис. Д.40.1.3.

БЕЗПЕКА ДАНИХ У NOVELL NETWARE 4.x

Означення понять 'безпека даних' та 'система безпеки даних'. Захист даних від апаратних збоїв та поломок. Захист службових таблиць. Захищений режим записування на диск та використання області Hot Fix. Захист даних від помилок програмного забезпечення. Доменна архітектура пам'яті. Система простежування транзакцій. Захист даних від несанкціонованого доступу. Захист під час реєстрації у системі. Електронне підписування пакетів.Система архівування даних Novell Netware 4.x.

Гарантувати безпеку даних – це означає захистити дані від різних зовнішніх факторів, які можуть призвести до їхньої втрати або спотворення.

Система безпеки даних передбачає комплекс засобів, які реалізують захист даних від можливого спотворення чи втрати.

41.1. Причини порушень безпеки даних та загальні вимоги до системи захисту даних

Інформаційна система, яку будують з використанням ОС, має складну структуру. Завдання захисту даних вирішуються в багатьох підсистемах і ланках.

Загальним принципом тут є включення механізмів захисту у відповідні функціональні блоки, максимальне їх наближення до місць спотворення даних.

Зокрема, власні механізми захисту даних від спотворень під час передавання мають протоколи різного рівня. Сервери захищені засобами операційної системи тощо.

Операційна система Novell Netware 4.x має розгалужену систему засобів безпеки даних. Ми розглянемо тільки найважливіші її елементи, не наведені в інших розділах. Засоби захисту класифікують за можливими джерелами спотворень даних. Джерела можливого спотворення даних можна розділити на такі три групи:

- апаратні збої та поломки;
- помилки програмного забезпечення;
- несанкціонований доступ.

41.2. Захист від апаратних збоїв та поломок

Найчастіше трапляються такі апаратні збої:
- раптове вимкнення живлення сервера або робочої станції;
- вихід з ладу твердого диска сервера або його контролера;
- поява на твердому диску зіпсутих блоків, у які неможливо виконувати записування-читання інформації.

Для захисту від апаратних збоїв використовують такі вбудовані засоби Novell Netware 4.x:
- дзеркальний диск або його дублювання;
- захист службових таблиць;
- захищений режим записування на диск та використання області *Hot Fix*.

Використання дзеркального диска або його дублювання. Одним з найменш надійних, однак таким, що найінтенсивніше використовується, пристроєм комп'ютера є твердий диск. З метою зберегти інформацію у випадку аварії твердого диска використовують **дзеркальний диск** (disk mirroring), тобто два однакові тверді диски приєднують паралельно до одного контролера (рис. 41.1). Записування відбувається одночасно на обидва диски. Якщо один з них вийде з ладу, система попередить оператора, однак інформація збережеться.

Дублювання диска (disk duplexing) полягає у приєднанні двох однакових дисків до двох контролерів. Такий варіант надійніший, ніж просте дзеркальне використання диска.

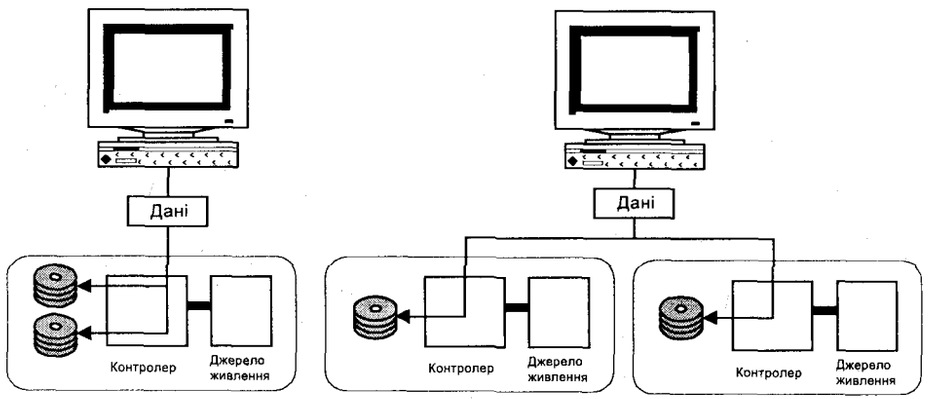


Рис. 41.1. Дзеркальне відображення та дублювання диска.

Захист службових таблиць. Важливими системними таблицями, які зберігають інформацію про розміщення каталогів та файлів, є DET- та FAT-таблиці. Якщо один з блоків диска,

де є ці таблиці, вийшов з ладу, багато інформації може стати недоступною. Щоб запобігти цьому, в системі зберігаються дві окремі копії цих таблиць. Якщо один з блоків таблиці зіпсутий, то система звертається до його копії. Номер зіпсутого блоку записується в таблицю зіпсутих блоків сервера і дані з нього зберігаються на диску у спеціально призначеній ділянці. Ідентичність DET- та FAT-таблиць перевіряється під час кожного вмикання сервера. У випадку розходження запускається утиліта ремонтування vrepair.

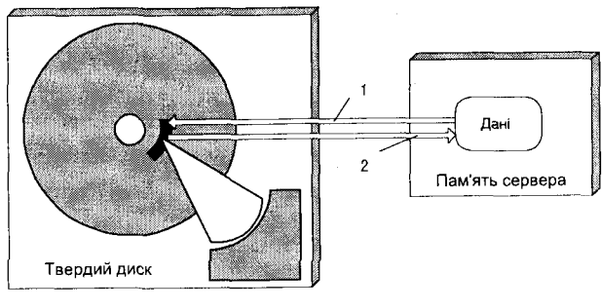


Рис. 41.2. Читання після записування: 1 – блок даних записується на диск; 2 – записані дані порівнюються з даними в ОП.

Захищений режим записування на диск та використання області Hot Fix. Унаслідок інтенсивних процесів записування та читання деякі блоки твердого диска можуть втратити можливість зберігати інформацію. Netware захищає дані від записування у такі блоки, використовуючи два механізми, які доповнюють один одного:
- читання після записування;
- використання області Hot Fix.

Відразу після записування даних у блок їх порівнюють з тими ж даними, які ще є у пам'яті (рис. 41.2). Якщо збіг повний, то пам'ять очищується, і система записує наступний блок. Якщо ж виявлено розходження, то блок вважається дефектним, і діє механізм використання області Hot Fix.

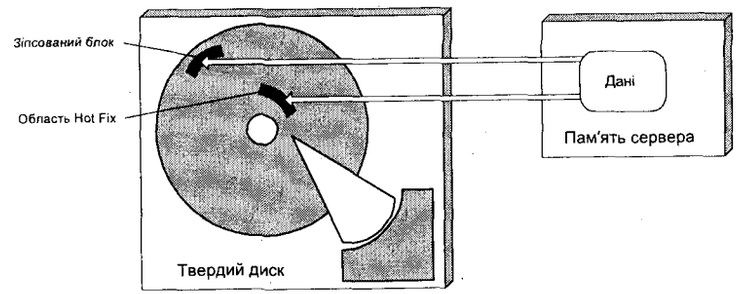


Рис. 41.3. Робота з областю Hot Fix.

Деяку частину твердого диска під час налаштування ОС резервують як область Hot Fix. За замовчуванням область Hot Fix займає 4% від ємності твердого диска. Під час налаштування системи її можна збільшити або зменшити. Блоки цієї області заміщують дефектні блоки диска. Якщо виявлено дефектний блок, він позначається як зіпсутий, і інформація з нього записується в блок, який належить області Hot Fix. Згодом у випадку звертання до зіпсутого блоку фактично буде відбуватися звертання до блоку в області Hot Fix (рис. 41.3).

41.3. Захист даних від помилок програмного забезпечення

Помилки програмного забезпечення призводять до 'зависання' комп'ютера, некоректного завершення програм і зумовленого цим порушення цілісності даних. Особливо небезпечною є некоректна робота програмного забезпечення сервера. Оскільки сервер працює одночасно з багатьма програмами, то спеціальний диспетчер розподіляє між ними пам'ять. Некоректно написаний модуль nlm (особливо створений іншими фірмами) може захопити пам'ять, яка належить іншій програмі, та наробити шкоди. Тому в Novell Netware 4.x є спеціальні механізми захисту пам'яті, побудовані з використанням концепції *доменної архітектури*.

Іншим потужним механізмом, який реалізовано в Novell Netware 4.x для захисту даних користувача як від апаратних, так і від програмних помилок, є *система простежування транзакцій (Transaction Tracking System (TTS))*.

Захист пам'яті. Для захисту пам'яті в Novell Netware 4.x використано апаратно реалізовану змогу процесорів Intel, починаючи з 486, поділяти пам'ять на окремі зони (0, 1, 2, 3). В ОС застосовують тільки зони з номерами 0 та 3. У зоні 0 (незахищеній) розміщена операційна система, у зоні 3 (захищеній) – програми користувачів. Незахищена (супервізорна) зона не має обмежень на ємність пам'яті, захищена (користувацька) такі обмеження може мати.

*Зони називають **доменами**. Архітектура використання пам'яті побудована на концепції доменів, називається **доменною**.*

Уся інформація, яку генерують відповідні програми, зберігається в межах домену, в якому розміщені програми.

Під час роботи розподіл пам'яті сервера відбувається динамічно. Межа між зонами пам'яті сервера рухома та переміщується залежно від потреб кожної зони. Якщо трапився збій у роботі програми захищеної зони, межа фіксується і аварійний nlm не може забрати пам'ять у супервізорної зони.

Система простежування транзакцій захищає результати роботи програм баз даних, вчасно поновлюючи попередній стан файлів баз даних, якщо виникла системна помилка. Простежування транзакцій є стандартною ознакою Novell 4.x, її можна ввімкнути або вимкнути.

Навіть якщо на сервері нема баз даних, TTS все-таки є корисною, оскільки захищає бази NDS та файли черг до ресурсів.

Останнім часом багато СКБД мають механізми захисту та поновлення транзакцій. Як звичайно, вони реалізовані на рівні СКБД. У Novell 4.x ця операція діє на рівні операційної системи. Такий підхід дає багато переваг, зокрема:

- всі транзакції відбуваються на сервері. Зменшується кількість інформації, яку передають мережею. Механізм транзакцій використовує Novell'івський кеш;
- підтримка програм, які не мають вбудованих механізмів опрацювання транзакцій. Якщо програма блокує файл бази або його запис, то операційна система вважає це початком транзакції.

Коли блокування припиняється, вважають, що транзакція успішно закінчилася.

Причини порушення даних можуть бути такі:

- вимкнення живлення сервера або робочої станції під час транзакції;
- збій апаратного забезпечення сервера або робочої станції (наприклад, помилка парності або адаптера мережі);
- 'зависання' сервера або станції під час транзакції (збій програмного забезпечення);
- збій або поломка апаратної компоненти мережі.

У випадку збою сервера попередній стан баз даних поновлюється під час поновного його ввімкнення. Якщо трапився збій робочої станції, TTS виконує поновлення негайно.

Захист TTS діє тільки для файлів баз даних, деяких застосувань електронної пошти та інших файлів, які побудовані з записів.

TTS гарантує, що будь-яка зміна файлу або відбувається повністю, або не відбувається взагалі. Для того, щоб увімкнути для файлу TTS, треба задати для нього атрибут *Transactional*. Такий файл не можна знищити або перейменувати.

На початку транзакції сервер робить копію файлу. Після цього відбуваються зміни в головному файлі. Коли транзакція закінчується, файл копії знищують.

Оскільки деякі застосування роблять деякі записи постійно блокованими (звичайно для захисту від копіювання), у Novell Netware 4.x можна задати межу блокування – кількість блокованих записів, при якій починає працювати TTS.

41.4. Захист даних від несанкціонованого доступу

Для захисту даних від несанкціонованого доступу в Novell Netware 4.x є ціла система, яку зручно розділити на такі компоненти:

- захист під час реєстрації у системі (login security) – обмежує коло осіб, які можуть увійти в систему;
- визначення довірених осіб – обмежує коло користувачів, які мають доступ до певного файлу, каталогу або об'єкта NDS;
- список прав – визначає рівень доступу та специфічні операції, які можна виконувати з даними;
- спадковість прав – передає права з верхніх рівнів ієрархії на нижні;
- атрибути – описують операції, які можна виконувати з файлами або каталогами незалежно від прав конкретного користувача;

• ефективні права – вислідні права, які формуються як комбінація призначених, успадкованих, групових та еквівалентних прав;

• розпізнавання (authentification) – перевіряє правомірність кожної операції між клієнтом та сервером, запобігає втручанню зловмисника під час транзакції;

• електронне підписування пакетів – запобігає підміні пакетів, які передають мережею;

• контролювання (audit) діяльності системи. Дає змогу незалежним від адміністратора аудиторам перевіряти діяльність усієї системи або її частини з метою відшукання незапланованих або несанкціонованих подій.

Захист під час реєстрації у системі дає змогу входити в систему тільки повноправному користувачу, який знає ім'я, контекст та пароль конкретного об'єкта типу *Користувач*. Подальші обмеження щодо входження у систему можна задати у властивостях користувацького об'єкта. Такими обмеженнями можуть бути час та місце реєстрації, період дії бюджету користувача, потреба періодичної зміни пароля, обмеження щодо мінімальної довжини пароля.

Деякі користувачі постійно дають одні й ті ж паролі. Щоб запобігти цьому, Novell Netware 4.x пам'ятає вісім останніх паролів для кожного користувача і не допускає їх повторного використання.

Паролі зашифровані і не висвітлюються на екрані та ніколи не передаються мережею (тому їх не можна перехопити). Пароль може підтверджувати кожну дію користувача.

Розпізнавання – це перевірка того, чи має об'єкт, який надсилає запит на якусь послугу, право на неї.

Крім обмежень на входження у мережу та прав доступу, воно гарантує безпеку у мережі. Єдиною операцією розпізнавання, яку бачить користувач, є введення ним пароля під час реєстрації в системі. Решта операцій виконується прозоро.

Процес обміну ключами під час входження в систему зображено на рис. 41.4. У цьому випадку використана комбінація локального ключа станції та загального ключа сервера. Процес складається з таких етапів:

• користувач надсилає своє ім'я серверу;

• сервер надсилає на станцію зашифрований локальний ключ;

• станція використовує пароль для дешифрування локального ключа та локальний ключ для побудови ідентифікатора; ідентифікатор надсилає серверу;

• сервер використовує загальний ключ для дешифрування ідентифікатора; якщо все правильно, сервер дозволяє станції працювати.

Така система називається системою кодування з загальним ключем. Ключі – це послідовності символів, які використовують у складних математичних формулах. Жоден з ключів не передають мережею в незашифрованому вигляді. Ключі не змінюються тільки під час конкретного сеансу роботи користувача. У найгіршому випадку, якщо перехоплено ключ, перехопленою буде інформація тільки з цього сеансу.

Електронне підписування пакетів. Одним із засобів боротьби з несанкціонованим доступом є електронне підписування пакетів, реалізоване для базового протоколу Netware (NCP).

Без такого підписування зловмисник може втрутитись у процес передавання, перехопити та підмінити пакет. Крім того, він може підмінити пакети адміністратора або іншого повноважного користувача та виконати дії з керування системою.

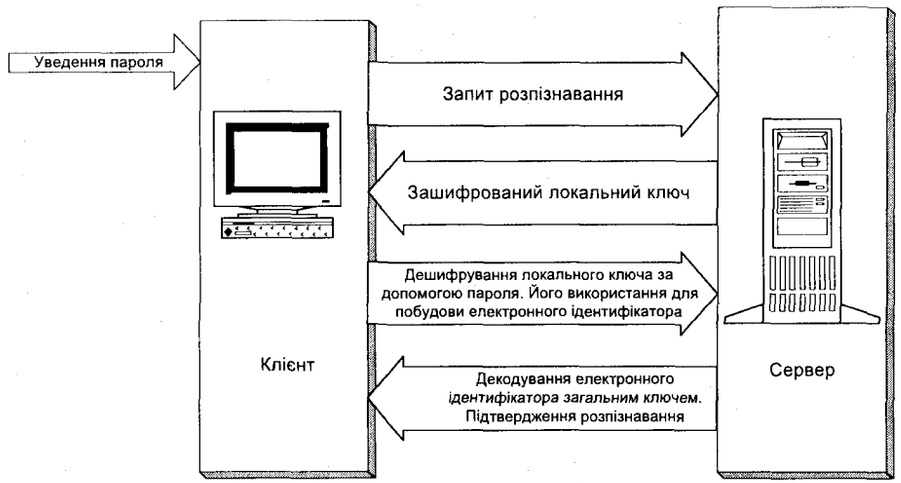


Рис. 41.4. Послідовність операцій розпізнавання.

Механізм електронного підписування передбачає, що клієнт (робоча станція) та сервер підписують пакети в процесі обміну, змінюючи підпис для кожного пакета. Пакети з неправильними підписами відкидаються, інформація про це надходить у файл помилок клієнта та на консоль сервера.

Цей механізм потребує затрат ресурсів центрального процесора. Тому систему підписів розробили гнучкою, щоб дати змогу вибрати потрібний ступінь захисту. Є чотири рівні підписування (0, 1, 2, 3). За замовчуванням діє рівень 1, який з мінімальною затратою ресурсів не вимикає захист. Рівні задають для сервера і кожної станції індивідуально у файлі net.cfg:

0 – пакети не підписують;

1 – клієнт підписує пакет тільки тоді, коли сервер цього вимагає (сервер має рівень 2 і більше);

2 – клієнт підписує пакет, якщо його може підписувати сервер (сервер має рівень 1 або більше);

3 – клієнт підписує пакети та вимагає щоб їх підписував сервер; якщо сервер пакети не підписує, відбувається розірвання сполучення.

Для сервера визначення рівнів підписування аналогічне. Поведінка системи у випадку різних взаємних співвідношень рівнів підписування для сервера та клієнта наведена в табл. 41.1.

Таблиця 41.1. Рівні підписування пакетів

	S=0	S=1	S=2	S=3
CI=0	Без підпису	Без підпису	Без підпису	Без вмикання
CI=1	Без підпису	Без підпису	Підпис	Підпис
CI=2	Без підпису	Підпис	Підпис	Підпис
CI=3	Без вмикання	Підпис	Підпис	Підпис

Конкретне співвідношення рівнів підписування для сервера та клієнта вибирають з міркувань забезпечення достатнього рівня захисту та мінімальних додаткових витрат ресурсів.

• Якщо вся інформація на сервері конфіденційна, треба задати як для сервера, так і для клієнтів рівень підпису 3.

• Якщо на сервері є як конфіденційна, так і загальнодоступна інформація, її поміщають у різні каталоги. Для сервера визначають рівень підпису 2, для клієнтів конфіденційної інформації – 3, звичайної – 1.

• Якщо користувачі часто змінюють станції, а на сервері є деякі конфіденційні дані, то рівень підпису сервера – 3, клієнта – 1.

• Якщо в мережі є загальнодоступна станція, а на сервері – деякі конфіденційні дані, то рівень підпису сервера – 3, а випадкового клієнта – 0.

Контролюванням (audit, ревізування) називається процес стеження за діяльністю користувачів (процесів та операцій у мережі) з метою забезпечення цілісності, секретності інформації.

Люди, які контролюють, діють незалежно від адміністраторів та інших користувачів мережі. Як звичайно, вони не мають права змінювати якісь параметри системи, а тільки файли контролю. Розглянемо події в мережі, які може контролювати аудитор.

• Щодо файлової системи:
  • створення, змінення, знищення каталогів або файлів;
  • перенесення, поновлення або перейменування каталогів або файлів;
  • створення та знищення черг на обслуговування.
• Щодо сервера:
  • вивантаження сервера;
  • створення або знищення об'єктів bindery;
  • монтування та демонтування томів;
  • зміна прав безпеки.
• Щодо NDS:
  • створення або знищення об'єктів;
  • перенесення та перейменування об'єктів;

  • зміна параметрів еквівалентності прав;
  • простеження входів та виходів користувача з системи.

Контролювання для файлової системи дозволене на рівні сервера, а для NDS – на рівні контейнера. Інформація з контролювання автоматично заноситься у текстові файли контролювання.

41.5. Система архівування даних Novell Netware 4.x

Архівування даних є важливою складовою частиною системи безпеки. Його треба виконувати періодично. В операційній системі Novell Netware 4.x є складна та потужна система архівування даних.

Розробники цієї системи поставили собі за мету створити єдину систему автоматичного архівування даних великої мережі з багатьма різними серверами, розподіленими базами даних, різними операційними системами робочих станцій. Запропоновану систему назвали **SMS** (Storage Management Service). SMS – це набір API, який ізолює застосування резервного копіювання від деталей реалізації Netware. Він працює незалежно від типу пристроїв архівування та операційних систем станцій.

SMS має таку структуру:

• **SBACKUP** – програма, яка керує резервним копіюванням;

• **SMDR** (Storage Management Data Requester) є посередником між SBACKUP та TSA. Водночас реалізує стандартний набір команд керування TSA, що дає змогу замість SBACKUP використовувати програми архівування, розроблені іншими фірмами;

• **TSA** (Target Service Agent) передає запит на архівування відповідному пристрою, приймає від нього інформацію і повертає SMDR. Є такі різновиди TSA: сервера Netware, віддаленого сервера, робочої станції, бази даних NDS та ін;

• **SDI** (Storage Device Interface) передає команди та інформацію між SBACKUP і пристроями архівування;

• драйвери пристроїв архівування. Кожен конкретний пристрій має свій драйвер. Драйвери керують простими механічними та електричними операціями пристрою;

• **Workstation Manager (WM)** розміщений на сервері та простежує факт увімкнення робочої станції, для якої треба зробити архівування по мережі.

Процес архівування дещо відрізняється для сервера, віддаленого сервера, робочої станції та бази даних NDS.

Під час архівування сервера SBACKUP дає запит на архівування до SMDR, який відшукує потрібний TSA і звертається до нього. TSA читає дані та повертає їх SBACKUP. SDI аналізує наявність пристроїв архівування даних та пропонує список таких пристроїв адміністратору. Вибравши пристрій, SBACKUP через SDI записує інформацію. SDI звертається безпосередньо до драйверів, які керують механічними операціями пристрою (такими як позиціонування головки, перемотування стрічки, завантаження диска тощо) (рис. 41.5). Читання інформації відбувається аналогічно.

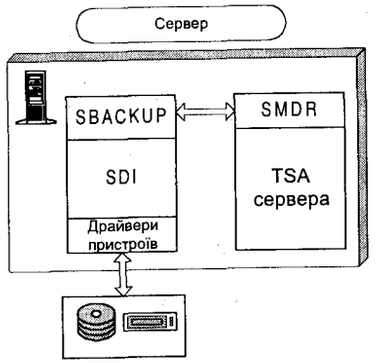


Рис. 41.5. Архівування локального сервера.

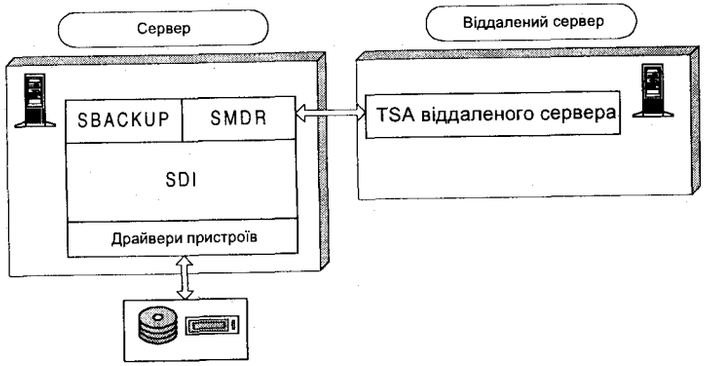


Рис. 41.6. Архівування віддаленого сервера.

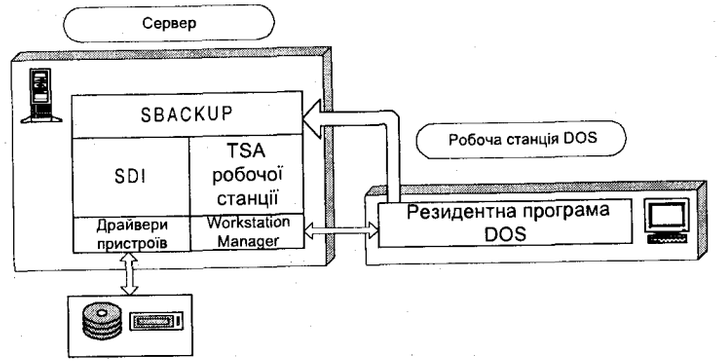


Рис. 41.7. Архівування робочої станції.

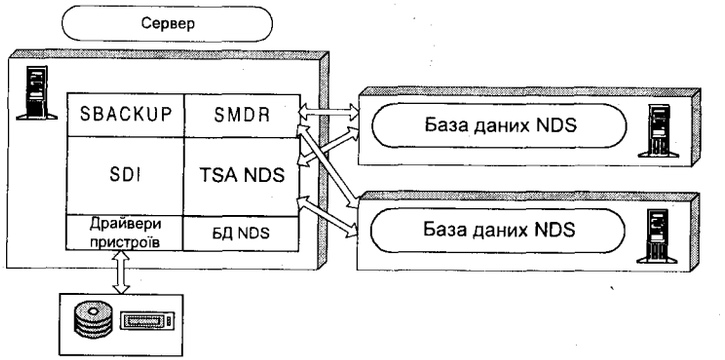


Рис. 41.8. Архівування бази даних NDS.

Архівуючи віддалений сервер, SBACKUP видає запит на архівування до SMDR. SMDR звертається до TSA на віддаленому сервері й одержує від нього дані для архівування. У всьому іншому цей процес аналогічний до архівування локального сервера (рис. 41.6).

Для архівування робочої станції на сервері запускають програму SBACKUP. Вона звертається через TSA до WM. Коли робоча станція завантажується, у її пам'яті з'являється спеціальна резидентна програма, яка відразу повідомляє WM про факт увімкнення станції (WM зберігає список усіх увімкнених станцій). WM одержує від резидентної програми станції порції інформації для архівування та передає їх через TSA SBACKUP, яка, відповідно, звертається до SDI. Записування інформації в ланці SBACKUP–SDI відбувається так само, як у попередніх випадках (рис. 41.7).

У процесі архівування бази даних NDS SBACKUP звертається через SMDR до TSA NDS. TSA NDS одержує дані з бази даних NDS, яка може одночасно бути розташована на кількох серверах, та передає їх SMDR. Подальші операції такі ж, як у інших випадках (рис. 41.8).

Бібліографія та джерела

Ценк А. Novell Netware 4.x К.: BHV, 1996.

ДРУКУВАННЯ В ОС NOVELL NETWARE 4.x

Загальна схема організації друкування. Об'єкти: черга на друкування, принтер, сервер друкування. Налагодження та головні властивості. Робота з системою друкування.

42.1. Загальна схема організації друкування

Операційна система Novell Netware 4.x має потужні засоби для організації мережевого друкування. Зокрема, вона дає змогу керувати виконанням завдань з друкування через властивості відповідних об'єктів NDS.

Головні принципи організації мережевого друкування описані в розділі 33. Однак для операційної системи Novell Netware 4.x ця схема значно ускладнена, зокрема, використано такі типи об'єктів NDS:

- сервер друкування;
- черга на друкування;
- принтер.

Сервер друкування обслуговує черги друкування. Кожному такому серверу як об'єкту NDS, фізично відповідає програмний модуль, що завжди розміщений на сервері Netware 4.x. На одному сервері можна запустити кілька серверів друкування. Кількість їх обмежена тільки наявними ресурсами пам'яті сервера. Серед властивостей сервера друкування є його ідентифікаційні дані (назва та розміщення), принтери, а також ідентифікатори операторів та користувачів, що працюють з сервером.

Черга на друкування зберігає завдання з друкування. Фізично цій черзі відповідає каталог на визначеному томі Netware 4.x. Черги на друкування можна створювати в томах різних серверів, іноді для цього формують окремий том. Отже, черга на друкування фактично є спулом, де розміщені невиконані завдання. Припинення роботи принтера може призвести до переповнення тому, в якому виділено чергу. Черга на друкування обслуговує принтери. Одному принтеру може бути призначено кілька черг, а одній черзі – кілька принтерів.

Об'єкт **принтер** ставить у відповідність певному реальному принтеру мережі його черги на друкування. Фізично мережеві принтери можна приєднувати до серверів Netware, робочих станцій, а також безпосередньо до мережі через мережевий адаптер.

Схема варіантів організації мережевого друкування показана на рис. 42.1. Сервер друкування завантажується на сервері Netware 4.x у вигляді модуля pserver.nlm. Він може керувати

друкуванням і на принтерах, приєднаних до інших серверів і робочих станцій. Для керування принтером, що приєднаний до сервера, використовують програму *nprinter.nlm*. Якщо ж принтер приєднано до робочої станції, то застосовують програму *nprinter.exe*, запущену на робочій станції.

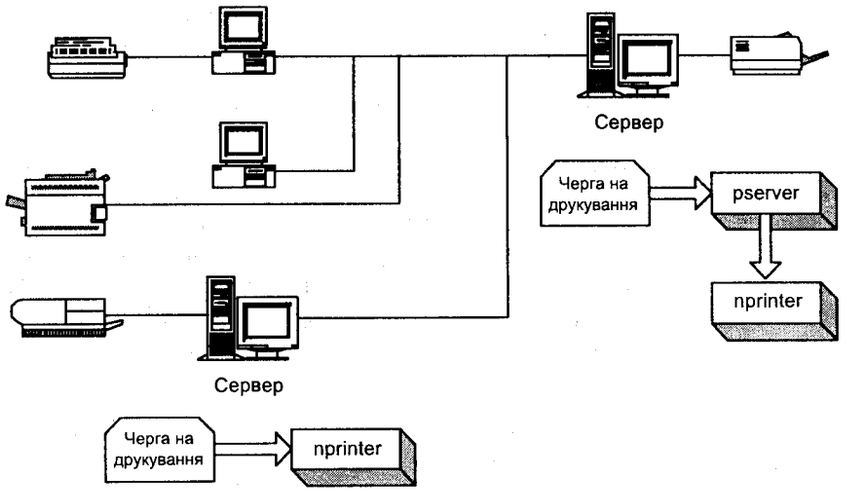


Рис. 42.1. Загальна схема організації друкування.

42.2. Налаштування системи мережевого друкування та керування нею

Для налаштування системи мережевого друкування потрібно виконати таке:

- визначити потрібну кількість об'єктів *черга на друкування*, *принтер*, *сервер друкування* та контексти їх розміщення;
- створити об'єкти *черга на друкування* та визначити їхні властивості;
- створити об'єкти *принтер* та визначити їхні властивості;
- створити об'єкти *сервер друкування* та визначити їхні властивості;
- визначити властивості об'єктів типу *користувач* та *організація* (*підрозділ*), що пов'язані з організацією друкування;
- запустити програми серверів друкування на відповідних серверах Novell Netware;
- запустити програми підтримки друкування на серверах та робочих станціях Novell Netware.

Планування системи друкування. Перед початком налаштування системи друкування треба ретельно її спланувати, тобто визначити потреби у друкуванні, кількість та розміщення

мережевих принтерів, з'ясувати їхні технічні параметри, визначити осіб, яким буде дозволено керувати кожним принтером, та осіб, яким дозволено користуватись ним.

Крім того, потрібно визначити кількість черг на друкування, оцінити їхній максимальний розмір та вирішити, на якому томі якого сервера розмістити кожну чергу, прикріпити до черги принтери.

Нарешті, треба визначити кількість серверів друкування та сервери Novell Netware, де будуть встановлені сервери друкування. Кожен сервер друкування займає частину пам'яті (по 20 Кб пам'яті на кожен принтер). Інтенсивна робота сервера друкування сповільнює виконання ним інших функцій. Один сервер друкування може обслуговувати до 256 принтерів.

Визначення черг на друкування. Нову чергу на друкування створюють як кожний новий об'єкт NDS. Якщо в мережі вже визначені принтери та сервери друкування, можна переглянути та задати деякі інші властивості черги. Якщо чергу створюють першою, то досить визначити тільки її ім'я та том розміщення. Черга має властивості *Оператори* та *Користувачі*.

Оператори – це список об'єктів типу *користувач*. Відповідні користувачі мають право знімати завдання на друкування з черги, змінювати його пріоритет, тимчасово блокувати.

У списку *Користувачі* є об'єкти типу *користувач*, власники яких мають право користуватися чергою на друкування.

Визначення об'єктів типу *принтер*. Під час створення об'єкта *принтер* визначають його ім'я, ідентифікаційну інформацію (опис, інші назви, розміщення, відділ, організація), мережеву адресу (задає система).

Тут також задають список черг на друкування, які обслуговує принтер, і присвоюють кожній черзі свій пріоритет. Одна з черг є чергою за замовчуванням. Завдання з цієї черги виконуватимуться, якщо в командах переспрямування друкування буде вказано лише принтер.

Властивостями *Конфігурації* є технічні параметри принтера, які можна налаштувати. Це тип порту, до якого приєднано принтер (паралельний, послідовний, інший), тип та форма заголовка, який автоматично роздруковується спочатку, інтервал опитування черги на друкування, розмір буфера друкування в кілобайтах, обмеження на адреси станцій, яким дозволено обслуговувати принтер.

Властивості *Повідомляти (Notification)* визначають користувачів та цілі контейнерні об'єкти, яким треба повідомляти про виникнення проблем (паперу нема або він перекошений, вимкнутий принтер та ін).

Налаштування об'єкта типу *сервер друкування*. У процесі визначення об'єкта *сервер друкування* задають його ім'я та визначають властивості, які згруповані за розділами *Ідентифікація*, *Призначення*, *Оператори*, *Користувачі*.

Ідентифікація дає змогу задати та переглянути такі властивості:

• ім'я сервера друкування (з цим іменем сервер відомий як об'єкт NDS);

• його advertising-ім'я (з цим іменем сервер відомий службам мережі як постачальник послуг друкування); для зручності ці два імені задають однаковими;

• інші назви, опис, версія, розміщення, підрозділ та організація;

• статус сервера (працює, вивантажений); спеціальна кнопка дає змогу користувачу з відповідними повноваженнями вивантажити сервер;

• кнопка налагодження пароля на сервер; якщо пароль задано, користувач зможе запустити сервер, якщо попередньо введе правильний пароль.

Група *Призначення* визначає для сервера закріплені за ним об'єкти-принтери. Кожен принтер одержує номер (від 0 до 255).

Властивості *Оператори* відповідає список об'єктів-користувачів, яким надано статус оператора сервера. Оператор може завантажувати та припиняти роботу сервера, переглядати його статус, керувати роботою принтерів сервера. Змінювати параметри сервера він не може, оскільки для цього потрібні відповідні права на об'єкт *Сервер друкування*.

Об'єкти зі списку *Користувачі* можуть переглядати всю інформацію про статус сервера друкування, однак не можуть робити змін. За замовчуванням у списку користувачів завжди є об'єкт-контейнер, де розміщено сервер друкування так, що всі користувачі цього контейнера автоматично одержують статус користувача.

Щоб роздрукувати свою інформацію, не обов'язково бути користувачем сервера, достатньо бути користувачем відповідної черги на друкування.

42.3. Робота з системою друкування мережі Novell Netware 4.x

Завантаження серверів та програм підтримки друкування. Після того, як система друкування у вигляді відповідних об'єктів NDS з визначеними властивостями сформована, можна приступати до роботи.

На визначеному сервері Novell Netware 4.x завантажують сервер друкування командою

```
load pserver [ім'я сервера друкування].
```

Якщо це ім'я не задане, виводиться меню, з якого можна вибрати один визначений сервер. Команду завантаження сервера вводять у командному рядку або записують у командний файл autoexec.ncf.

Якщо до сервера Novell Netware 4.x приєднано принтер, то для його обслуговування треба завантажити в пам'ять спеціальну програму

```
load nprinter advertising_ім'я_сервера номер принтера.
```

Якщо ж принтер приєднано до робочої станції DOS, то потрібно завантажити в пам'ять станції програму керування принтером nprinter.exe. Для кожного приєднаного принтера завантажують окрему програму.

Робота з чергою друкування. У системі друкування, що працює, можна переглянути список завдань на друкування для кожної визначеної черги. Приклад списку показано на рис. 42.2.

Print Queue: HP6 Print Queue

Print Jobs: 5

Seq	Job Name	Description	Form	Status	Job ID
001	Admin	Autoexec.bat	0	Ready	00C48001
002	Admin	config.sys	0	Ready	00C3B002
003	Admin	text.txt	0	Ready	00C3C003
004	b_user	iogtext.log	0	Ready	01C3F005
005	Guest	proba.doc	0	Ready	01C3F004

Рис. 42.2. Список завдань на друкування.

У цьому списку відображено послідовний номер завдання, ім'я користувача – власника завдання, опис завдання, форму друкування, яку використовують, статус завдання (Ready – є в черзі, Held – завдання тимчасово блоковане). Кнопки керування чергою дають змогу оператору зняти завдання на друкування, затримати його або переглянути детальні параметри.

До детальних параметрів завдання належать кількість копій, задання форми друкування, заголовка (banner), порядкового номера завдання у черзі, режиму повідомлення власника про закінчення друкування та ін.

Робота з принтером. Під час роботи системи друкування можна переглянути параметри принтера в його об'єкті. Параметри є такі:

- назва черги, яку обслуговує в цей час принтер;
- назва та номер завдання на друкування;
- номер форми, кількість копій;
- розмір документа в байтах;
- відсоток виконання.

Користувач може припинити друкування, знову розпочати його, використати певну форму, зняти завдання з друкування.

Спрямування завдань на друкування. Якщо користувач працює з застосуваннями, що безпосередньо підтримують роботу в операційній системі Novell Netware 4.x, він може попередньо не закріплювати портів своєї станції за принтерами. В іншому випадку йому доведеться звернутися до команди capture, яка має такий формат:

capture [p=ім'я принтера| q=ім'я черги на друкування] [параметри...].

Ця команда ставить у відповідність одному з локальних портів друкування (параметр l=n) мережеве ім'я принтера або черги на друкування. Вона діє на рівні DOS. Якщо наявний один з параметрів (принтер або черга), інший вибирається за замовчуванням. Команда має велику кількість параметрів, які дають змогу конфігурувати завдання на друкування. Кожен користувач, підрозділ чи організація можуть задати свою конфігурацію. Для цього є група властивостей *Конфігурація завдання на друкування*.

Керування завданнями на друкування. Під час переглядання завдань на друкування виводиться таблиця з іменами завдань та їхніх власників. Кожне завдання має такі властивості:

- ім'я;
- ім'я принтера або черги на друкування, для яких визначена конфігурація;
- визначення *пристрою друкування*;
- кількість копій, потреба друкувати заголовок;
- позначення порту локального принтера.

Ці властивості відповідають параметрам командного рядка **capture**. Для однієї черги на друкування можна визначити багато завдань на друкування.

Робота з означеннями *пристроїв друкування*. Кожен принтер, як звичайно, має свої команди керування, які дають змогу задати початковий стан, вибрати шрифт, інтервал та ін. Для динамічного керування принтером під час друкування та з метою використати набори вбудованих команд кожної марки принтера використовують механізм *пристроїв друкування*. У комплекті постачання ОС є понад 50 означень пристроїв друкування, проте користувач може задати свої. Процес визначення пристрою друкування має кілька стадій.

Спочатку визначають послідовності команд керування для окремих функцій друкування (початковий стан, грубий шрифт тощо). Кожній функції дають назву. Далі з визначених функцій будують режими функціонування пристрою як набір функцій. Кожен з режимів також одержує назву. Режими та функції групують у списки для кожного пристрою.

Пристрої друкування визначають на рівні контейнера. Під час роботи станції можна надсилати певні набори команд на принтер, посилаючись на ім'я пристрою друкування та режиму в конфігурації завдання на друкування.

Бібліографія та джерела

Ценк А. Novell Netware 4.x. К.: BHV, 1996.

МЕРЕЖЕВІ АСПЕКТИ ОС UNIX

Загальна характеристика та історія розвитку. Головні архітектурні принципи побудови Unix. Файлова система. Типи файлів. Монтування та демонтування. Головні системні таблиці. Адміністрування та захист даних Unix. Комунікації в Unix.

43.1. Загальна характеристика та історія розвитку

Операційна система Unix була розроблена в 70-х роках для роботи на великих та середніх ЕОМ у термінальному режимі з розподілом часу. Це багатокористувацька, багатопроцесна, багатозадачна система. Unix працює в режимі витіснення з диспетчеризацією.

Порівняно з ОС Novell Netware Unix має зовсім іншу філософію обслуговування користувачів. Якщо Novell Netware передбачала виконання головних функцій на комп'ютері клієнта, а сервер спочатку надавав тільки послуги зі спільного використання файлів та принтерів, то Unix працювала тільки з неінтелектуальними текстовими dumb-терміналами в режимі розподілу часу центрального процесора між ними. Такі термінали передавали на сервер тільки коди натиснутих клавіш, а вся обчислювальна робота відбувалась на центральному комп'ютері. Не дивно, що такий комп'ютер у системі Unix називали *гост* (host – головний, хазяїн). З появою персональних комп'ютерів Unix-системи стали використовувати ресурси ПК (переважно для роботи клієнтської частини в застосуваннях архітектури *клієнт–сервер*), однак головна частина опрацювання даних і надалі відбувається на сервері. Сьогодні Novell Netware є найліпшим файл-сервером, а Unix – найліпшим сервером застосувань.

43.2. Головні архітектурні принципи побудови Unix

Головні компоненти Unix-системи такі:

• **Ядро.** Виконує всі системні функції. Воно постійно перебуває в оперативній пам'яті і завантажується туди після ввімкнення комп'ютера. Ядро оформлене як виконавчий файл. Під час будь-якого переналаштування системи, введення нових драйверів, зміни параметрів генерації системи ядро перебудовується і зберігається у наново створеному файлі. Функції ядра відображені на рис. 43.1.

• **Оболонка – інтерпретатор команд** (shell). Призначений для сприйняття, інтерпретування та передавання ядру для виконання команд мови керування Unix. Фактично виконує інтерфейсні, посередницькі функції між ядром та прикладними програмами.

• **Прикладні програми.** Звертаються до інтерпретатора команд та ядра системи.

Рис. 43.1. Функції ядра Unix.

Базовою концепцією організації обчислень в Unix є поняття процесів. Процес – це програма, яка виконується. Процес завжди створюється іншим процесом і зберігає ідентифікатор батьківського процесу. Під час створення нового процесу створюють і деяку віртуальну машину, що його виконує. Процеси в Unix незалежні, але можуть взаємодіяти під час виконання. Ядро системи обслуговує багато незавершених процесів. Кванти часу процесора кожному процесу виділяє диспетчер Unix почергово.

> *У випадку перемикання системи між різними процесами, якщо в пам'яті не вистачає місця, відбувається* ***переписування*** *(swapping) найстаршого процесу на твердий диск і вивільнення місця в пам'яті для нового процесу. Сьогодні переписування поступилось ефективнішому* ***пейджингу*** *(paging), який на твердий диск переписує не весь процес, а тільки деякі його сторінки.*

Система запам'ятовує активний стан програми та даних для всіх незавершених процесів і поновлює їх по черзі. Процеси можуть породжувати інші процеси. Кожен процес має свій ідентифікатор.

Інформація про процеси у вигляді відповідних дескрипторів зберігається в таблиці процесів. Сучасні версії Unix дають змогу зберігати в такій таблиці кілька сотень процесів.

Один з процесів працює постійно. Він має ім'я **init**. Якщо класифікувати процеси Unix, то можна виділити користувацькі та системні, а також процеси-демони (daemons). Більшість процесів має статус користувацьких. Системні – це процеси, орієнтовані на виконання системних функцій, найчастіше звертання до ядра системи як до певної підпрограми. Якщо користувацькому процесу треба виконати системну функцію, він формує системний виклик. З моменту генерації системного виклику процес стає системним. Як бачимо, користувацький та системний процеси – це часто дві фази одного й того ж процесу. Процеси-демони є різновидом системних процесів, які виконуються у фоновому режимі. Вони виконують системні дії, пов'язані з обслуговуванням мережі (так звані listener'и, протоколи), адмініструванням ресурсів (фонове записування та оновлення даних) та ін.

Отже, архітектура Unix дає змогу сформувати розподілену систему як сукупність процесів, що обмінюються даними. Для обміну інформацією між процесами Unix пропонує використання:

- сигналів;
- семафорів;
- програмних каналів;
- черг повідомлень;
- сегментів пам'яті, що розділяється;
- спеціальних команд (write, cu, mail);
- засобів міжмашинної взаємодії (uucp, tcp/ip, nfs, rfs).

Техніка передавання сигналів між процесами формує реакцію системи на деякі події (натискання на клавіші, знищення процесу, зменшення напруги мережі електроживлення, деякі помилки та збої). Реакція системи на визначені події передбачена за замовчуванням, однак користувач може перехопити таке 'переривання' і написати свою програму опрацювання переривання.

Семафори – це цілі числа або масиви цілих чисел, які дають змогу організувати коректний доступ до ресурсів системи, які треба використовувати в монопольному режимі. Семафор може тимчасово припинити процес, якщо потрібний йому ресурс зайнятий.

Програмні канали (pipes) – це засіб комунікації між процесами, який дає змогу процесам, що виконуються у системі, обмінюватись інформацією, синхронізувати роботу, працювати як одне ціле. Програмний канал – це деякий спеціальний файл, над яким дозволені операції читання та записування. Спроба записування в канал, для якого нема читання, призведе до затримки процесу-записувача аж доки не з'явиться процес-читач і навпаки. Для введення-виведення з каналу використовують потокову модель даних. Дані не інтерпретуються і їхня довжина ніяк не обмежена. Визначають неіменовані та іменовані програмні канали. Неіменовані програмні канали налагоджують тільки між процесами-родичами. Іменовані канали можна налагоджувати між довільними процесами. Однак кожний канал є між парою процесів.

Черги повідомлень, як і програмні канали, є засобом взаємодії процесів, однак допускають гнучкішу організацію такої взаємодії. Для черг не обов'язкова наявність пари процесів записувач-читач, просто є деяка черга повідомлень, до якої у разі потреби звертаються процеси записувачі і читачі. Для формування черги не використовують потокову модель даних. Кожне повідомлення має структуру (тип та дані). У ньому можуть бути довільні дані. Розмір повідомлення обмежений загальним розміром черги, заданим у момент її створення. Його можна читати з черги у довільному порядку. Багато процесів можуть працювати з однією чергою.

Техніка **пам'яті спільного використання** дає змогу значно пришвидшити обмін даними. У всіх попередньо розглянутих випадках обмін даними відбувався за посередництвом ядра системи. У разі використання спільної пам'яті обмін даними відбувається шляхом записування-читання даних у виділену частину віртуального адресного простору. Для синхронізації взаємодії багатьох процесів з пам'яттю спільного використання застосовують семафори.

43.3. Файлова система Unix

Типи файлів та структура файлової системи. Основою файлової системи Unix є файл. Означені такі типи файлів:

- звичайні дискові файли;
- каталоги;
- спеціальні файли.

Важливим принципом організації файлової системи є те, що доступ до зовнішніх пристроїв реалізовано через файли.

Файли зберігаються на диску як послідовність байтів. Система не накладає обмежень на їхню структуру та зміст. Цю структуру інтерпретує відповідна програма опрацювання файлу. Максимальна кількість файлів в одній файловій системі – 6500.

Текстові файли мають визначений формат – окремі рядки розділені символами переведення рядка.

Каталог – це файл спеціального формату, який містить записи про файли каталогу. Кожен запис каталогу складається з назви файлу та посилання на його індексний дескриптор. Unix дає змогу робити кілька посилань на один і той самий файл, розміщуючи для кількох файлів посилання на один і той же індексний дескриптор.

Індексний дескриптор – це запис у таблиці індексних дескрипторів, який містить системну інформацію про файл.

Спеціальний файл є посередником між процесом користувача та драйвером відповідного пристрою, що розміщений у ядрі системи та опрацьовує звертання програми згідно з вимогами певного пристрою.

Монтування та демонтування файлової системи. Одну файлову систему завжди монтують у кореневому каталозі root. Її неможливо демонтувати.

Монтування та демонтування файлової системи треба розуміти так само, як монтування тому Netware. Змонтувати файлову систему означає завантажити її системні таблиці у пам'ять: файлова система стає 'видимою' для операційної системи.

Файловій системі у фізичному сенсі відповідає твердий диск або його частина. Твердий диск можна поділити на розділи і кожен з них можна монтувати як окрему файлову систему. Нову файлову систему монтують у точці монтування, якій відповідає каталог уже змонтованої файлової системи. Для монтування та демонтування використовують команди mount та umount:

mount файл_пристрою каталог_монтування.

Можливість монтування файлових систем використовують не тільки для приєднання додаткових твердих дисків, але і для монтування віддалених файлових систем, систем інших типів (наприклад Netware) (див. розділ 44).

Зміст та структура системних таблиць. Перший блок файлової системи – це блок початкового завантаження. Якщо файлова система допускає завантаження, то в цьому блоці міститься програма-завантажувач, яка читає ядро та розміщує його у пам'яті. Ядро та деякі інші системні програми розміщені у спеціальному каталозі.

У другому блоці диска міститься заголовок та головна інформація файлової системи (розмір та кількість вільних блоків, загальна кількість індексних дескрипторів та ін.) Далі записують блоки, в яких розміщено список індексних дескрипторів. Кожен запис списку зберігає інформацію про один файл (режим, тип файлу, його довжина в байтах, ідентифікатори власника та групи, дата останньої модифікації). Довжина індексного дескриптора – 64 байти. Найважливіша частина дескриптора – це список адрес блоків на диску, де зберігається файл. Він складається з 13 номерів блоків. Перші 10 номерів означають адреси перших десяти блоків файлу. Одинадцятий блок містить посилання на блок, де розміщені наступні 256 адрес блоків файлу, дванадцятий – адресу блоку, який містить адреси ще 256 блоків, кожен з яких містить адреси 256 блоків файлу, тринадцятий – систему непрямого посилання третього рівня. Отже, максимальний розмір файлу в Unix – 16842762 блоки або 17246988288 байти.

43.4. Адміністрування та захист даних в Unix

Unix має елементи захисту на рівні користувачів та їхніх груп. Користувачів системи створює адміністратор. Він визначає login-ім'я користувача та його пароль.

Усі користувачі системи зберігаються у файлі /etc/passwd. Тут також у зашифрованому вигляді зберігаються паролі. Один користувач з номером 0 є привілейованим адміністратором системи і має доступ до всіх файлів. Групи, їхній склад зберігаються у файлі /etc/group.

З кожним процесом асоційовано два ідентифікатори: ідентифікатор користувача та ідентифікатор групи. Для процесів, запущених на виконання командою командного рядка, ідентифікатори користувача та групи одержують з реєстраційної інформації користувача, для інших процесів копіюються аналогічні параметри батьківського процесу.

З кожним файлом також асоційовані ідентифікатори користувача та групи. Файл успадковує ці параметри від процесу, який його створив. Ідентифікатори файлу визначають права доступу до нього для трьох категорій користувачів:

- власника файлу;
- членів групи власника файлу;
- інших користувачів.

Кожен файл має свій код захисту, який присвоюють йому під час створення. Код захисту – це слово в індексному дескрипторі файлу з заданими значеннями бітів.

000400 – читання власнику;
000200 – записування власнику;
000100 – виконання власнику;
000040 – читання членам групи;
000020 – записування членам групи;
000010 – виконання членам групи;
000004 – читання іншим користувачам;
000002 – записування іншим користувачам;
000001 – виконання іншим користувачам;
004000 – дозвіл змінити ідентифікатор користувача;
002000 – дозвіл змінити ідентифікатор групи.

Дозвіл змінити ідентифікатор користувача або групи дає змогу прикладній програмі тимчасово поміняти власника файлу і забезпечити доступ до файлів даних та інших програм від імені цього власника. Це гарантує, що з даними працюватимуть тільки за посередництвом прикладної програми.

Захист інформації в Unix є на таких рівнях:

- захист під час входження в систему;
- захист файлів.

Реєструючись у системі, користувач уводить своє ім'я та пароль. Пароль зберігається у файлі /etc/passwd і користувач може в будь-який момент його змінити.

Певні слабинки системи Unix дають змогу або розшифрувати паролі (якщо є вихідний код системи чи доступ до файлу паролів), або підставити термінальну програму getty і прочитати пароль з екрана.

43.5. Утиліти та програми передавання інформації. Комунікації в Unix

В основі комунікацій Unix є протокольний стек TCP/IP, демони якого працюють у фоновому режимі. Організація комунікацій відповідає загальній філософії Unix: нема якоїсь однієї, центральної програми комунікації, а є великий набір утиліт, кожна з яких виконує визначені функції. Всі утиліти, як звичайно, запускають тільки з командного рядка, вони мають силу-силенну ключів та параметрів і не дуже дружній інтерфейс. Водночас комунікації органічно вписані в концепцію цієї ОС, яка з самого початку повинна була підтримувати розподілені конфігурації користувачів та ресурсів.

Розглянемо головні утиліти та програми комунікацій.

Утиліти ping, telnet, ftp найчастіше застосовують користувачі Unix.

Утиліта ping призначена для перевіряння наявності зв'язку з певною машиною у мережі. Найчастіше її використовують для визначення цілісності мережі. Формат команди:

ping адреса госта | ім'я госта.

Утиліта telnet – це програма емуляції термінала. Її запуск дає змогу працювати на ПК як на терміналі Unix. Ця програма належить до базового сервісу Unix і добре працює не тільки в локальних мережах, а й в сполученнях на велику відстань.

Програма ftp призначена для копіювання файлів на віддалену машину та навпаки. Запускають її так:

ftp ім'я госта.

Унаслідок розпочнеться сеанс роботи з ftp. Під час цього сеансу можна, використовуючи команди

put ім'я файлу або get ім'я файлу.

передати або одержати файли з віддаленої системи. Закінчують ftp-сеанс командою

bye.

Утиліти uucp, cu, uucico та ін. Група утиліт uu- призначена для організації обміну інформацією в мережі машин Unix (яку ще називають Usenet). Сюди належать утиліти uucp, uucheck, cu, uuname, uucleanup, uushed, uustat, uulog, uutry, uuto, uugetty, uux, uuxqt.

Кожна машина в мережі Unix має своє унікальне ім'я. Утиліта uuname виводить список усіх відомих системі імен.

Утиліта cu налагоджує між двома машинами дуплексний комунікаційний канал. Інформація читається зі стандартного пристрою введення однієї машини і передається на іншу. Одночасно інформація від іншої машини приймається та виводиться на стандартний пристрій виведення. Формат команди

cu [-sшвидкість] [-iлінія] [ключі] номер телефону | ім'я машини.

Утиліту uucp використовують для копіювання файлів з однієї Unix-системи на іншу. Формат команди

uucp [ключі та параметри] файл1 [файл2...] файл призначення.

Ім'я файлу записують або як повне маршрутне ім'я на локальній машині, або складають з імені машини та маршрутного імені для ідентифікації віддаленої системи. Назву машини відділяють знаком оклику. Наприклад, uunet!/cat1/user/file1.

Командою uux збирають файли з різних машин, виконують над ними дії на вказаній машині і передають результати у заданий файл на якійсь з машин. Для виконання цієї команди треба мати відповідні повноваження на всіх залучених машинах.

Утиліта uuxqt обслуговує запити з виконання завдань на локальній машині від віддаленої машини. Вона переглядає виділений для виконуваних файлів каталог та відшукує вказану програму, виконує її, а результат спрямовує запитувачу.

Програма електронної пошти Mailx одна з найскладніших і часто уживаних програм Unix. Вона має текстовий рядковий інтерфейс та орієнтована для роботи на терміналах і ПК в режимі термінала. Якщо система електронної пошти налагоджена на комп'ютері, то функціонує

демон пошти. Поштовий демон приймає та передає повідомлення у фоновому режимі. У разі вмикання комп'ютера він приймає адресовану йому пошту з інших машин.

Прийняту локальну пошту скеровують в індивідуальну для кожного користувача поштову скриньку, оформлену у вигляді файлу. Якщо скринька не порожня, то система дає користувачу повідомлення:

you have mail.

Для того, щоб відіслати повідомлення пошти, треба знати login-ім'я адресата та його адресу, яку можна задати у форматі мережі Usenet або Internet. Наприклад, команда формування листа може бути такою:

mail txt!domingo,
mail icmman!uscsi!iris!lot!diva!mozart.

У другому випадку маємо приклад передавання листа через багато машин-посередників (multihop mail). Поштова команда з Internet-адресою виглядає так:

mail mozart@terra.icm.com.

У цьому випадку в адресі є ім'я користувача, імена госта, підмережі та домену (DNS-ім'я).

Якщо не задано імені файлу, повідомлення вводять зі стандартного джерела (клавіатури). Спочатку пишуть тему повідомлення (Subject), потім його текст. Система дає змогу вибрати тему повідомлення як відповідь на одержаний Subject або навіть відповідь на відповідь.

Для одержання електронної пошти користувачу треба набрати команду і переглянути список одержаних повідомлень, зазначивши відправника та тему. Він може переглянути повідомлення вибірково або по черзі. Переглянуте повідомлення має статус прочитаного. Користувач може перевести його у свій власний поштовий каталог у вигляді окремого файлу або ж знищити. Деякі поштові системи автоматично знищують прочитані повідомлення під час виходу з програми пошти.

Бібліографія та джерела

1. *Дунаев С.* Unix System V. Release 4.2. Общее руководство. М.: Диалог-МИФИ, 1995.
2. *Немет Э., Снайдер Г., Сибасс С., Хейн Т.* Unix: руководство системного администратора. К.: BHV, 1997.

ПОБУДОВА МУЛЬТИПРОТОКОЛЬНИХ СИСТЕМ ТА ВЗАЄМОДІЯ МЕРЕЖЕВИХ ОС

Загальна характеристика принципів побудови мультипротокольних систем. Підходи та програмні продукти організації взаємодії мереж Netware та Unix. Мультиплексування протокольних стеків. Рівні мультиплексування. Менеджери протоколів.

Сучасні комп'ютерні мережі, як звичайно, гетерогенні і містять багато серверів, що працюють на різних ОС (Netware, Unix, Windows NT), та багато клієнтів (DOS, Windows, Unix, Windows NT, Macintosh). Системний інтегратор повинен забезпечити взаємодію цих різнорідних систем у єдиній інформаційній системі підприємства.

44.1. Загальна характеристика принципів побудови мультипротокольних систем (на прикладі Novell Netware, Unix та Windows NT)

Організація спільної роботи в одній мережі комп'ютерів кількох різних операційних систем у сучасному розумінні зводиться до побудови мультипротокольних систем.

> ***Мультипротокольною*** *називатимемо систему, в якій одночасно підтримуються кілька різних протокольних стеків.*

Мультипротокольність забезпечують трьома різними шляхами.

• Розробка та використання окремих програмних продуктів, спеціально призначених для організації доступу між двома різними системами. У такому підході нема універсальності.

• Встановлення кількох протокольних стеків на одній (або обох) з машин, які беруть участь у взаємодії. Такий підхід називають мультиплексуванням протокольних стеків. Комп'ютери з різними протокольними стеками обирають для взаємодії протокол, зрозумілий іншим учасникам обміну.

• Налаштування спеціального компонента мережі – шлюзу, на якому встановлено обидва протокольні стеки. Шлюз транслює протоколи одного стека в інший. Процедура транслювання має евристичний характер, оскільки не завжди є однозначна відповідність між двома протоколами. Особливо це стосується різних методів адресації ресурсів.

У реальних мережах сьогодні використовують усі три підходи, однак найчастіше – другий.

44.2. Використання спеціальних програмних засобів

Розглянемо використання спеціальних програмних засобів на прикладі організації сполучення мереж Novell Netware та Unix.

За рівнем функціональних можливостей розрізняють кілька класів продуктів та функцій.

• **Емуляція терміналів** у Novell Netware. У цьому випадку персональний комп'ютер – робоча станція Netware – перетворюється в алфавітно-цифровий термінал Unix. Не використовують ресурси ПК, проте користувач має доступ до госта Unix, його мережевих можливостей. Функцію емуляції терміналів, як одну з примітивних, реалізують багато пакетів програм (*Lan Workgroup*, *Microsoft TCP/IP*).

• **Емуляція сервера Novell Netware.** Цю функцію реалізують продуктом **Netware for Unix**. Файлову систему Netware монтують на гості Unix як одну з його файлових систем. Клієнти Netware бачать цю файлову систему як ще один сервер Netware. Користувачі Unix, зареєстровані як користувачі обох ОС, працюють з файловою системою Netware як з файловою системою Unix. Аналогічну, однак розширену, функцію виконує і продукт Novell *NFS-Gateway*. Приєднані до якогось сервера Netware клієнти працюють з усіма файловими системами Unix як з томами Netware-сервера.

• **Емуляцію госта Unix** реалізують програмою *NFS-server*. Її налаштовують на сервері Netware. Клієнти бачать цей сервер як гост Unix.

• **Використання механізмів NFS.** Для віддаленого доступу до госта Unix можна застосувати програми та підходи продукту **NFS**, розробленого фірмою Sun Microsystems. Для цього в файлі /etc/exports можна задати каталоги, доступні всім NFS-клієнтам, або змонтувати віддалений каталог як окрему файлову систему своєї машини.

Для сполучення ОС Unix та Windows NT можна застосувати такі продукти:

• програмний продукт **Samba**, який налаштовують на сервері Unix, надаючи змогу користувачам різних варіантів ОС Windows (що працюють з файловим протоколом SMB) мати доступ до інформації цього сервера;

• продукт NFS, який у цьому випадку налаштовують як на сервері Unix, так і клієнті Windows NT.

44.3. Мультиплексування протокольних стеків

Засоби мультиплексування протоколів для зручності прийнято розміщувати на трьох рівнях:

• під час реалізації драйверів адаптерів (на канальному рівні);

• у програмах, що працюють на мережевому і транспортному рівнях;

• на серверах та редиректорах (сеансовий, рівень відображення та прикладний).

Для організації мультиплексування на кожному з цих трьох рівнів уводять **мультиплексер (менеджер) протоколів**. Головна його функція – створення єдиного інтерфейсу доступу до різних протоколів з боку протоколів верхнього рівня, вибір та перемикання між протоколами.

У Windows NT один мережевий протокол може використовувати кілька драйверів канальних протоколів, а один драйвер адаптера може працювати з кількома мережевими протоколами. На найнижчому рівні застосовують драйвер, написаний відповідно до специфікації NDIS (рис. 44.1). Мультиплексер NDIS ізолює драйвер мережевого адаптера від апаратури. Windows NT підтримує також і мультиплексер ODI (в ОС Netware таким мультиплексером є програма lsl).

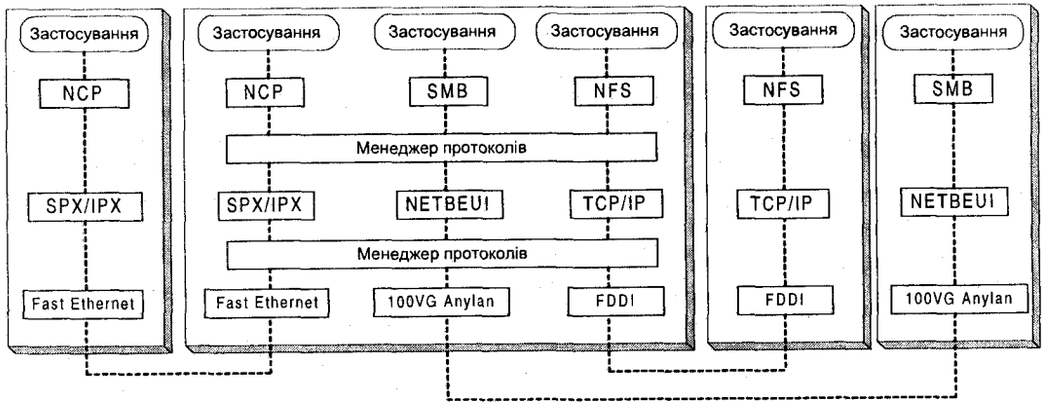


Рис. 44.1. Мультиплексування протоколів у Windows NT.

На середньому рівні вводять стандарт на інтерфейс транспортних засобів TDI. У Windows NT ці протоколи реалізовані у вигляді драйверів уведення-виведення. Редиректори та транспортні протоколи, написані відповідно до правил TDI, можуть створювати довільні зв'язки між собою. Для доступу до функцій транспортного рівня використовують інтерфейси Netbios та Windows Sockets, які звертаються до транспортних протоколів через інтерфейс TDI. Поряд з TDI застосовують також і модифіковане середовище STREAMS, розроблене для Unix.

На верхньому рівні у Windows NT є два мультиплексери – **MUP** та **MPR**. Кожен мультиплексер вирізняється своїм сценарієм доступу до мережевого ресурсу.

У першому випадку застосування звертається до операційної системи з запитом, у якому є назва мережевого ресурсу у форматі *Універсального Формату Імені (Universal Naming Convention (UNC))*. Наприклад,

\\icm_server\C$\Ox\text.doc.

Якщо під час аналізу ім'я файлу наведене в UNC-форматі, викликається MUP, який його опрацьовує. MUP визначає належність імені до однієї з доступних мереж, звертаючись до всіх цих мереж. Редиректор шукає ресурс і повідомляє MUP. Визначене співвідношення кешується і наступного разу шукання не відбувається.

Згідно з другим сценарієм, застосування спочатку відображає мережевий ресурс на локальний, а потім звертається до нього як до локального ресурсу. Наприклад, UNC-ім'я \\icm_server\C$\Ox\text.doc відображається на диск F:. Перед закріпленням мережевого ресурсу за локальним відбувається перегляд мережевих ресурсів. Netware 3.11 для цього використовує протокол SAP, редиректор у Novell Netware 4.x – довідкову службу NDS. У Windows NT список доступних серверів надає компонента *Computer Browser*, а список каталогів визначають у результаті діалогу редиректора та сервера за протоколом SMB. У мережах Unix (TCP/IP) послуга щодо перегляду мережевих ресурсів взагалі не передбачена й адресу ресурсу завжди треба задавати явно. MPR реалізована у вигляді бібліотеки *.dll. MPR мультиплексує зв'язки між застосуваннями і кількома редиректорами різних мереж. Він взаємодіє з редиректорами через посередників (network provider) (рис. 44.2).

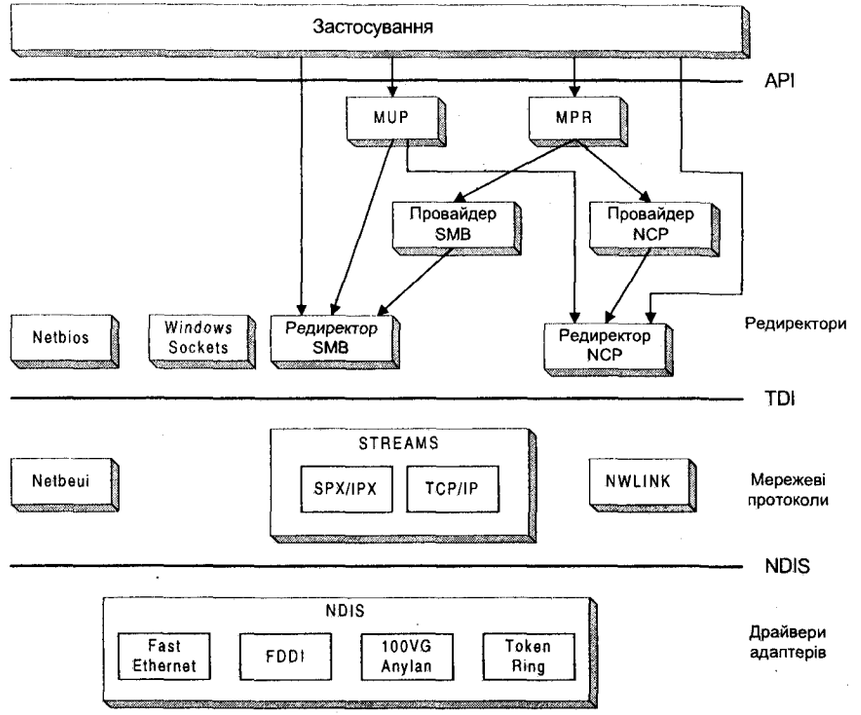


Рис. 44.2. Робота мультиплексерів.

44.4. Використання граничних шлюзів

У випадку використання граничних шлюзів додаткове програмне забезпечення шлюзу ставлять тільки на машині шлюзу (клієнти та сервер не змінюються). Водночас шлюз працює повільніше, ніж мультиплексер протоколів.

Для зв'язку з Novell Netware у Windows NT є програма шлюзу *Gateway Service for Netware*. У цьому випадку клієнти NT не налаштовують редиректори Netware, а звертаються до сервера Netware за допомогою протоколу SMB. Каталоги Netware виглядають для них як каталоги локального сервера.

Недоліком є те, що для зв'язку створюють одного користувача Netware з відповідним набором повноважень. Цей набір діє для всіх клієнтів NT, що сполучаються з сервером Netware.

Бібліографія та джерела

1. *Гантер Д., Барнет С., Гантер Л.* Интеграция Windows NT и Unix в подлиннике. СПб.: BHV, 1998.
2. *Гаскин Д.И.* Интеграция Unix и сетей Netware. Руководство Novell. М.:Лори, 1994.
3. *Олифер Н., Олифер В.* Не имей сто друзей, а имей Windows NT // LAN Magazine. 1996. № 5.

Перелік уживаних скорочень*

АС абонентська система
АС автономна система
АТС автоматична телефонна станція
АЦП аналого-цифровий перетворювач
БД база даних
ВК вузол комутації
ГМ глобальна мережа
ЕОМ електронна обчислювальна машина
ІКМ імпульсно-кодова модуляція
КМ комп'ютерна мережа
ЛМ локальна мережа
МДКН метод доступу з контролем сигналу-носія
МДКН/ВК метод доступу з контролем сигналу-носія і виявлянням колізій
МККТТ Міжнародний консультативний комітет з телеграфії та телефонії
МФЛ модем для фізичних ліній
МТС Міжнародний Телекомунікаційний Союз
ОС операційна система
ПБП протокол багатопакетного передавання
ПВМП протокол великих міжмережевих пакетів
ПЗ програмне забезпечення
ПЗП постійна пам'ять
ПК персональний комп'ютер
РІС розподілена інформаційна система
РП регістр передавання
РРС радіорелейна станція
СК служба каталогів
СКБД система керування базами даних
СПД сервісний пункт доступу
УКХ ультракороткі хвилі
ФС файлова система
ЦАП цифро-аналоговий перетворювач
ЦП центральний процесор

AAL (ATM Adaptation Layer) рівень адаптації ATM
ACL (Access Control) керування доступом
ACK (Acknowledgement) (біт) підтвердження отримання
ACL (Access Control List) список керування доступом
AD (Active Directory) служба каталогів
ADCP (Advanced Data Communicatio Protocol) удосконалений протокол обміну даними
ADSL (Asymmetrical Digital Subscriber Line) асиметрична цифрова абонентська лінія (зв'язку)
AEIA (American Electronics Industries Association) Американська асоціація електронної промисловості
AM (Active Monitor) активний монітор
AMPS (Advanced Mobile Phone Service) удосконалена служба мобільного зв'язку
ANSI (American National Standard Institute) Американський національний інститут стандартів
API (Application Program Interface) інтерфейс прикладних програм
ARP (Address Resolution Protocol) протокол перетворення IP-адреси в канальну

* Уклав О.Коссак

ASCII (American Standard Code for Infomation Interchange) американський стандартний код обміну інформацією
ASMP (Asymetrical Multiprocessing) асиметричне мультипроцесорне опрацювання
ATA (AT Attachment) інтерфейс приєднання пристроїв IDE до комп'ютера AT
AT (Attention) увага
AT (Advanced Technology) передова технологія
ATA (AT Attachment) інтерфейс приєднання пристроїв IDE до комп'ютера AT
ATAPI (ATA Package Interface) пакетний інтерфейс для ATA
ATM (Asynchronous Transfer Mode) режим асинхронного передавання
AUI (Attachment Unit Interface) інтерфейс сполучення робочої станції з приймачем-передавачем
BBS (Builten Board System) електронна дошка оголошень
BECN (Backward Explicit Congestion Notification) повідомлення (біт) про зворотне ущільнення
BFT (Binary File Transfer) передавання двійкового файлу
BGP (Border Gateway Protocol) протокол зовнішньої маршрутизації
BIOS (Basic Input/Output System) базова система введення-виведення
BISDN (Broadband ISDN) широкосмугова цифрова мережа ISDN
BOOTP (Boot Protocol) протокол автоматизованного завантаження комп'ютера
BRI (Basic Rate Interface) інтерфейс базового доступу (користувача в ISDN)
BSC (Binary Synchronous Communication) двійкове синхронне передавання
BSC (Byte Sequence Control) керування послідовністю байтів
CBR (Constant Bit Rate) стала бітова швидкість
CCITT (Consultative Comittee on Telegraphy and Telephony) Міжнародний консультативний комітет з телеграфії та телефонії
CCTA (Central Computer and Telecomunications Agency) Центральна агенція з питань комп'ютерів та телекомунікацій
CDMA (Code Division Multiple Access) груповий доступ з кодовим розподілом каналів
CDPD (Cellular Digital Packet Data) стандарт цифровового пакетного передавання даних у стільникових мережах
CEC (Commission of European Communities) Комісія Європейської Спільноти
CIR (Commited Information Rate) гарантована швидкість передавання (інформації)
COM (Component Object Model) об'єктна модель компонентів
CRC (Cyclic Redundancy Check) циклічний контроль надлишковим кодом
CRS (Configuration Report Server) сервер звітів про конфігурації
CS (Convergence Sublayer) підрівень конвергенції
CSLIP (Compressed Serial Line Interface Protocol) міжмережевий протокол для послідовного каналу зі стисканням
CSMA (Carrier Sense Multiple Access) груповий доступ з контролем сигналу-носія
CSMA/CD (Carrier Sense Multiple Access with Collision Detection) груповий доступ з контролем сигналу-носія і виявлянням колізій
CUG (Closed User Group) закрита група користувачів
DCE (Data Communication Equipment) апаратура передавання даних
DCOM (Distributed COM) розподілена об'єктна модель компонентів
DDB (Digital Data Bus) шина цифрових даних
DDP (Distributed Data Processing) розподілене опрацювання даних

DET (Directory Entry Table) таблиця доступу до каталогів
DFC (Data Flow Control) керування потоком даних
DHCP (Dynamic Host Configuration Protocol) протокол динамічного налаштування комп'ютера
DLC (Data Link Control) керування каналом передавання даних
DLE (Data Link Escape) перехід до інших значень символів (символ керування)
DMA (Direct Memory Access) прямий доступ до пам'яті
DNS (Domain Name Service) протокол служби логічних імен
DOS (Disc Operation System) дискова операційна система
DPP (Demand Priority Protocol) протокол доступу з запитом пріоритету
DPSK (Different Phase Shift Keying) фазова модуляція
DS0 (Digital Sygnal level Zero) стандартний канал мовлення (64 Кбіт/с)
DSL (Digital Subscriber Line) абонентська лінія цифрового зв'язку
DSS (Direct Station Select) пряме обирання станції
DSS (Decision Support System) експертна система
DTE (Data Terminal Equipment) термінальне обладнання для передавання даних
DTI (Digital Trunk Interface) інтерфейс цифрового сполучення
DVMRP (Distance Vector Routing Protocol) протокол багатоадресної маршрутизації
EA (Extended Address) розширена адреса
ECMA (European Computers Manufacturers) Європейська асоціація виробників комп'ютерів
ED (End Delimiter) вказівник кінця (повідомлення)
EGP (Exterior Gateway Protocol) протокол зовнішньої маршрутизації
EIA (Electronic Industries Association) Асоціація електронної промисловості
EISA (Extended ISA) розширена шина ISA
EMI (Electromagnetic Interference) параметр випромінювання в довкілля
ENQ (ENQuiry) символ запиту
EOM (End of Message) кінець повідомлення
EOT (End of Transmission) кінець передавання
EPP (Enhanced Parallel Port) розширений LPT-порт (для приєднання комунікаційних адаптерів)
ESDI (Enhanced Small Device Interface) розширений інтерфейс малих пристроїв (дисків)
ETB (End of Transmission Block) кінець передавання блоку
ETS (Enhanced Throughput Cellular) удосконалений протокол для стільникових модемів
ETSI (Europian Telecommunication Standards Institute) Європейський інститут телекомунікаційних стандартів
ETX (End of Text) кінець тексту
FAT (File Allocation Table) таблиця розміщення файлів
FCC (Federal Communications Commission) федеральна комісія з комунікацій
FDDI (Fiber Distributed Data Interface) інтерфейс передавання розподілених даних волоконно-оптичними каналами
FDMA (Frequency Division Multiple Access) груповий доступ з розподілом частот
FECN (Forward Explicit Congestion Notification) повідомлення про пряме ущільнення
FIFO (First-In, First-Out) прийшов першим - вийшов першим
FLP (Fast Link Pulse Burst) пакет імпульсів контролю сполучення

FOIRL (Fiber Optic Inter-Repeater Link) волоконно-оптичний зв'язок між ретрансляторами
FQDN (Fully Qualified Domain Name) повне доменне ім'я
FR (Frame Relay) ретрансляція кадрів
FS (File Separator) розділювач файлів
FSK (Frequency Shift Keying) частотна модуляція
FTAM (File Transmission Application Method) протокол керування передаванням файлів
FTP (File Transfer Protocol) протокол передавання файлів
FTP (Folged Twisted Pair) фольгована скручена пара
GAN (Global Area Network) глобальна мережа
GSM (Global System for Mobile Communication) глобальна система мобільного зв'язку
HAL (Hardware Abstraction Layer) рівень апаратних абстракцій
HCSS (High Capacity Storage System) накопичувач великої ємності
HDLC (High-level Data Link Control) високорівневий протокол керування каналом зв'язку
HDSL (High bit rate Digital Subscribers Line) високошвидкісна цифрова технологія, яка використовує наявні мідні мережі
HEC (Header Error Correction) корекція помилок у заголовку
HST (High Speed Technology) високошвидкісна технологія
HTML (Hypertext Markup Language) мова опису гіпертекстових сторінок
HTTP (Hypertext Transfer Protocol) протокол передавання гіпертексту
IAB (Internet Activities Board) Комісія з питань діяльності Internet
ICMP (Internet Control Message Protocol) протокол для діагностування мережі
IDE (Intelligent Drive Equipment) інтелектуальне обладнання дискового накопичувача
IDL (Interface Definition Language) мова опису інтерфейсів
IEC (International Electrotechnical Commitee) міжнарожний комітет з електротехніки
IEEE (Institute of Electronical and Electrotechnical Engineers) Інститут інженерів електроніків та електротехніків
IETF (Internet Engineering Task Force) підрозділ інженерних розробок Internet
IGRP (Interior Gateway Routing Protocol) протокол внутрішньої маршрутизації для великих неоднорідних мереж
IMAP (Internet Message Access Protocol) протокол доступу до повідомлень (в Internet)
IO (Input/Output) уведення-виведення
IOS (Internetwork Operation System) міжмережева операційна система
IP (Internet Protocol) протокол міжмережевої взаємодії (в Internet)
IPX (Internet Datagram Protocol) дейтаграмний протокол передавання пакетів
IPX (Inter Packet eXchange) протокол (мережевого рівня) обміну пакетами
IRF (Inherited rights filter) фільтр успадкованих прав
IRTF (Internet Research Task Force) дослідницький підрозділ протоколів Internet
ISA (Industry Standard Architecture) промислова стандартна архітектура (тип системної шини)
ISDN (Integrated Services Digital Network) цифрова мережа інтегрованих послуг
ISO (International Standardization Organization) Міжнарожна організація зі стандартизації
ITU (International Telecommunication Union) Міжнародний Телекомунікаційний Союз
JTM (Job Transmission Method) протокол передавання завдань
LAN (Local Area Network) локальна мережа
LANE (LAN Emulation) емуляція ЛМ
LAP (Link Access Protocol) протокол доступу до каналу (зв'язку)

LAPD (Link Access Protocol D) протокол доступу до каналу D
LAPM (Link Access Procedure for Modem) протокол доступу до каналу (зв'язку) для модема
LBS (Local Bridge Server) сервер моста
LCW (Link Code Word) інформаційне слово
LD (Local Device) віддалений пристрій
LDM (Limited Distance Modem) модем для швидкісного передавання прямим кабелем
LEO (Low Earth Orbit) низькоорбітальний (супутник)
LIP (Large Internet Packets) протокол великих міжмережевих пакетів
LLAP (Local Talk Link Access Protocol) протокол доступу до каналу
LLC (Logical Link Control) керування логічним каналом
LP (Link Partner) віддалений партнер
LPC (Local Procedure Call) виклик локальних процедур
LSL (Link Support Layer) рівень підтримки сполучення
MAC (Media Access Control) керування доступом до середовища
MAN (Metropolitain Area Network) регіональна мережа
MAU (Media Access Unit) пристрій спряження
MAU (Multistation Access Unit) пристрій багатостанційного доступу
MCA (Micro Channel Architecture) мікроканальна архітектура (тип системної шини)
MCR (Minimum Cell Rate) мінімальна швидкість передавання комірок
MDI (Media Interface) інтерфейс з передавальним середовищем
ME Microsoft Exchange
MF Microsoft Fax
MIB (Management Information Base) інформаційна база для керування (маршрутизаторами і гостами мережі TCP/IP)
MII (Media Independent Interface) незалежний від носіїв інтерфейс
MIME (Multipurpose Internet Mail Extentions) протокол багатоцільового розширення для електронної пошти (в Internet)
MIR (Maximum Information Rate) максимальна швидкість передавання (інформації)
MLM (multilayer mapping) міжрівневе відображення
MOSPF (Milticast Open Shortest Path First) протокол багатоадресної маршрутизації
MPOA (Multiprotocol over ATM) стандарт передаваня інформації між віртуальними локальними мережами без використання маршрутизаторів
MPR (Multiple Provider Router) маршрутизатор множинних провайдерів (багатофункціональний драйвер обміну)
MS DOS (Microsoft Disc Operation System) дискова операційна система фірми Microsoft
MSN Microsoft Network
MUP (multiple UNC provider) провайдер множинних UNC
NAK (Negative Acknowledgement) підтвердження неотримання
NAL (Netware Application Launcher) середовище запуску застосувань
NAM (Netware Application Manager) менеджер застосувань
NAMPS (Narrowband AMPS) вузькосмугова удосконалена служба мобільного зв'язку
NDD (Netware Directory Database) розподілена база даних Netware
NDIS (Network Device Interface Specification) специфікація інтерфейсу мережевого адаптера
NDS (Netware Directory Services) служба каталогів Netware
NEC (National Electric Code) національний електричний стандарт

NETBEUI (NetBIOS Extended User Interface) розширений інтерфейс користувача NetBIOS
NetBIOS (Network BIOS) мережева базова система введення-виведення
NEXT (Near End Crosstalk) перехідне загасання на ближньому кінці
NIC (Network Information Center) центр розподілу адрес в Internet'і
NIC (Network Interface Card) мережевий адаптер
NLM (Netware Loadable Module) завантажувальний модуль Netware
NLP (Normal Link Pulse) імпульс контролю сполучення
NNI (Network Node Interface) інтерфейс вузлів мережі
NNTP (Network News Transport Protocol) мережевий протокол надавання новин
NP (Next Page) біт про обмін наступними інформаційними словами
NRZ (Non Return to Zero) без повернення до нуля
NUA (Network User Address) адреса абонента мережі
NUI (Network User Identity) ідентифікаційний номер абонента мережі
OC (Optical Carrier) волоконно-оптичний носій
ODI (Open Datalink Interface) відкритий інтерфейс каналу передавання даних (специфікація драйвера)
OSF (Open Software Foundation) фонд відкритих систем
OSI (Open Systems Interconnection) сполучення відкритих систем
OSPF (Open Shortest Pass First) протокол внутрішньої маршрутизації
PAD (Packet Assembler/Disassembler) конвертер пакетів
PBP (Packet Burst Protocol) протокол багатопакетного передавання
PC (Personal Computer) персональний комп'ютер
PCI (Peripherial Component Interconnect bus) шина взаємодії периферійних компонент
PCR (Peak Cell Rate) пікова швидкість передавання комірок
PCS (Physical Coding Sublayer) підрівень фізичних сигналів
PDA (Personal Digital Assistant) персональний цифровий секретар
PDC (Primary Domain Controller) головний контролер домену
PDS (Packet Driver Specification) специфікація драйвера пакетів
PIM (Protocol Independent Multicast) протокол багатоадресної маршрутизації
PMA (Physical Media Attachment) блок керування передаваннями та виявлення колізій
POP (Post Office Protocol) протокол електронної пошти
POSIX (Portable Operating System Interface) інтерфейс переносних операційних систем
PPP (Point-To-Point Protocol) протокол взаємодії між вузлами
PRI (Primary Rate Interface) магістральний інтерфейс (в ISDN)
PPTP (Point-to-Point Tunneling Protocol) протокол тунельної взаємодії між вузлами
PCS (Personal Communication Service) служба персонального зв'язку
PSC (Public Service Commission) Державне агентство телекомунікаційних послуг
PTS (Primary Time Server) первинний сервер часу
PVC (Permanent Virtual Channel) постійний віртуальний канал
QAM (Quadrature Amplitude Modulation) квадратурна амплітудна модуляція
QoS (Quality of Service) якість обслуговування
RARP (Reverse Address Resolution Protocol) протокол визначення за канальною адресою IP-адреси

REM (Ring Error Monitor) сервер помилок кільця
RF (Remote Fault) біт помилки приймання
RFC (Request For Comments) запит на пояснення
RIP (Routing Information Protocol) протокол внутрішньої маршрутизації для невеликих мереж
RISC (Reduced Instruction Set Computing) спрощена система машинних команд
RMI (Remote Method Invocation) виклик віддалених методів
RMON (Remote Monitoring Specification) протокол віддаленого керування мережею
RPC (Remote Procedure Call) виклик віддаленої процедури
RPS (Ring Parameter Server) сервер параметрів кільця
RS (Reconciliation Sublayer) підрівень узгодження
RTS (Reference Time Server) довідковий сервер часу
RTT (Round Trip Time) час поширення сигналу до одержувача та назад
SAR (Segmentation and Reassembly Sublayer) підрівень сегментації і реагрегування
SCR (Sustained Cell Rate) середня швидкість передавання комірок
SCSI (Small Computer System Interface) системний інтерфейс малих комп'ютерів
SDDI (Shielded Distributed Data Interface) розподілений інтерфейс передавання даних екранованою скрученою парою
SDLC (Synchronous Data Link Control) синхронне керування передаванням даних
SDN (Synchronous Digital Hierarhy) ієрархія синхронних цифрових (оптичних) каналів
SID (Security ID) ідентифікатор безпеки
SLIP (Serial Line IP) протокол передавання даних послідовним каналом
SM (Standby Monitor) пасивний монітор
SMB (Service Message Block) протокол передавання файлів
SMDR (Station Message Detail Reporting) облік телефонних переговорів
SMP (Symmetrical Multiprocessing) симетричне мультипроцесорне опрацювання
SMS (Storage Management Service) служба керування пам'яттю (система автоматичного архівування даних великої мережі)
SMTP (Simple Mail Transfer Protocol) простий протокол електронної пошти
SNMP (Simple Network Management Protocol) протокол керування мережею
SONET (Synchronous Optical NETwork) СОНЕТ (інтерфейс)
SPI (Service Provider Interface) інтерфейс драйвера служби
SPX (Xerox Sequenced Packet Exchange) протокол обміну послідовністю пакетів
SQL (Structured Query Language) мова структурованих запитів
SRTS (Single Reference Time Server) єдиний довідковий сервер часу
SST (Spread Spectrum Technology) технологія розподілу сигналу за спектром частот.
STP (Shielded Twisted Pair) екранована скручена пара
STP (Spanning Tree Protocol) протокол залишкового дерева
STS (Secondary Time Server) вторинний сервер часу
STS (Synchronous Transfer Mode) режим синхронного передавання
SVC (Switched Virtual Cirquit) комутований віртуальний канал
SVD (Simultaneous Voice and Data) модем одночасного передавання голосу та даних
TC (Transmission Control) керування передаванням
TCM (Trellis Coded Modulation) модуляція з гратковим кодуванням та уведенням надлишковості

TCP (Tramsmission Control Protocol) протокол керування передаванням (пакетів)
TDI (Transport Driver Interface) інтерфейс драйвера транспорту
TDMA (Time Division Multiple Access) груповий доступ з розподілом у часі
TDR (Time Domain Relectometer) рефлектометр (прилад для локалізації розривів електричних кіл)
TIA (Telecommunications Industry Association) Асоціація телекомунікаційної промисловості
TTS (Transaction Tracking System) система простежування транзакцій
UART (Universal Asynchronous Receiver/Transmitter) універсальний асинхронний приймач-передавач (мікросхема)
UDP (User Datagram Protocol) данограмний протокол
UL (Underwriters Laboratories) лабораторії сертифікації
UNC (Universal Naming Convention) універсальний формат імені
UNI (User to Network Interface) інтерфейс користувача з мережею
UPS (Uninterrupted Power Supply) джерело безперебійного живлення
URL (Uniform Resource Locator) уніфікований вказівник ресурсів
UTC (Universal Coordinated Time) скоординований всесвітній час
UTP (Unshielded Twisted Pair) неекранована скручена пара
UUCP (Unix-to-Unix Copy) копіювання (файлів) між Unix-системами
UUID (Universally Unique Identifier) унікальний ідентифікатор (сервера)
VBR (Variable Bit Rate) змінна бітова швидкість
VCI (Virtual Circuit Identifier) ідентифікатор віртуального каналу
VLAN (Virtial LAN) віртуальна мережа
VLM (Virtual Loadable Module) віртуальний завантажувальний модуль
VPI (Virtual Path Identifier) ідентифікатор віртуального шляху
VSAT (Very Small Aperture Terminal) наземна станція (супутникового зв'язку) з малою антеною
VTAM (Virtual Telecommunications Access Method) віртуальний телекомунікаційний метод доступу
VTSP (Virtual Terminal Service and Processing) протокол сервісу віртуального термінала
WAN (Wide Area Network) глобальна мережа
WOSA (Windows Open Services Architecture) відкрита архітектура Windows-послуг
WWW (World Wide Web) всесвітнє павутиння, Web-технологія (розподілена інформаційна технологія)

Предметний покажчик

Зміст

Наукове видання

Євген БУРОВ

КОМП'ЮТЕРНІ МЕРЕЖІ

Підп. до друку 12.05.99. Формат 70×90/16.
Папір офсетний. Гарн. Таймс. Друк офсетний.
Умови. друк. арк. 30,00. Умови. фарбовідб. 38,61.
Наклад 2500. Зам. 214-9.

СП «БаК»
а/с 9009, Львів 290011
тел. (0322) 72 67 50, 75 47 71
тел./факс (0322) 72 26 29

Львівська книжкова фабрика «Атлас»
вул. Зелена, 20, Львів 290005

R&M *freenet*

Оптимальна Структурована Кабельна Система для передавання мовлення, даних і відеозастосувань.

R&M пропонує повний спектр обладнання, яке відповідає вимогам до нових E і F Класів.

Нова структурована кабельна система R&M freenet забезпечує комплексне вирішення, необхідне для побудови найсучаснішої кабельної структури підприємства будь-якого рівня.

- Система включає компоненти Категорій 5e, 6, 7 і волоконно-оптичні (Клас D+, E і F).
- Широкий спектр обладнання для інтеграції мовлення.
- Підтримує оптичні і мідні середовища.
- Повний, модульний дизайн системи дає змогу легко нарощувати її можливості.
- Кольорове маркування призначене для легкої ідентифікації різних сервісів.
- Великий резерв щодо продуктивності (ACR).
- Нові волоконно-оптичні з'єднувачі LSH (E2000), SC-Compact, MT-RJ забезпечують дуплексне волоконно-оптичне вирішення в стандартному установному місці RJ45.

Разом з повним спектром обладнання R&M пропонує повний пакет висококваліфікованого сервісу:

- багаторівневу програму гарантій, аж до довічних;
- мережу сертифікованих R&M freenet інсталяторів;
- постійну підтримку з боку досвідчених спеціалістів R&M.

Вкладайте свої кошти в орієнтовані у майбутнє Кабельні Системи!
R&M надійний партнер.

Наша адреса:
Київ 252133, бульвар Лихачова, 1/27,
Тел./факс: +044 295 6969
E-mail: rdm@rdmua.com.ua
Одеса 270009, вул. Сонячна, 5,
Тел.: +0482 60 45 52
Факс: +0482 21 99 88
E-mail: rdmua@farlep.net
Internet: http://www.rdm.ch

R&M

Оптимальні вирішення для Ваших кабельних мереж